International Journal of Creative and Open Research in Engineering and Management
ISSN: 3108-1754 (Online)
Volume 02 Issue 10 October-2026 | Impact Factor: 3.5



# Hybrid Optimization-Driven Machine Learning for Intrusion Detection in Cloud Environments: A Systematic Literature Review

**Mitali Choudhary[1], Khushbu Tamrakar[2]**

[1,2] Oriental University, Indore

**How to Cite this Article**:

Choudhary, M. & Tamrakar, K. (2026). Hybrid Optimization-Driven Machine Learning for Intrusion Detection in Cloud Environments: A Systematic Literature Review. International Journal of Creative and Open Research in Engineering and Management, 02(10), 1-9. https://doi.org/10.55041/ijcope.v2i10.156

**License:**

This article is published under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are credited.

© The Author(s). Published by International Journal of Creative and Open Research in Engineering and Management.





https://doi.org/10.55041/ijcope.v2i10.156

## Abstract

Cloud computing has become the backbone of modern digital services, but its shared and distributed nature makes it an attractive target for cyber-attacks. Intrusion Detection Systems (IDS) built with machine learning and deep learning are now central to cloud security, and a large body of recent work tries to improve them with metaheuristic optimization for feature selection and model tuning. This paper presents a systematic literature review of hybrid optimization-driven machine learning frameworks for intrusion detection, with a focus on cloud and cloud-adjacent (IoT and IIoT) environments. Following a PRISMA-based review process, 30 peer-reviewed studies published between 2008 and 2026 were selected and analysed. The review organises the literature into four themes: cloud intrusion detection with feature selection, hybrid and improved metaheuristic optimization methods, CNN–LSTM and other optimized deep learning models, and foundational or survey work. A comparative analysis of the feature selection method, optimizer design, classifier type and data-balancing strategy used in each study is presented, along with the trend of publications over time. The review finds that although metaheuristic feature selection and CNN–LSTM classifiers are both well studied on their own, very few studies combine a hybrid dual-optimizer search with a CNN–LSTM classifier specifically for cloud network traffic, and fewer still report search overhead or explain their model's decisions. These gaps are summarised to guide future research and form the basis of an ongoing dissertation project.

***Keywords***—*Cloud security, Intrusion detection system, Systematic literature review, Feature selection, Metaheuristic optimization, Grey Wolf Optimizer, Particle Swarm Optimization, CNN–LSTM, Machine learning.*

## 1. Introduction

Cloud computing gives organisations on-demand access to computing, storage and software over the internet, and it now underlies services in banking, healthcare, education and e-commerce. This convenience comes at a cost: because many tenants share the same physical infrastructure, a single weak point can expose the data of many users, and cloud platforms are a constant target of denial-of-service attacks, probing, and unauthorised access attempts [1]. Firewalls, encryption and access control reduce the risk, but they cannot detect every attack, which is why an Intrusion Detection System (IDS) that continuously watches network traffic remains an essential second line of defence [1], [2]. Similar concerns apply to fog and edge nodes that extend the cloud closer to end devices, where lightweight anomaly-detection models have also been studied [3].

Traditional signature-based IDS tools compare traffic against a list of known attack patterns and cannot recognise a new or modified attack. Machine learning and deep learning based, anomaly-oriented IDS tools instead learn the normal pattern of traffic from data and flag anything unusual, which allows them to generalise to previously unseen attacks [1]. Two practical problems limit how well such models perform. First, network traffic is described by a large number of features, many of which are redundant or irrelevant, so an IDS built on the full feature set is slow and can be less accurate than one built on a carefully chosen subset. Second, attack records are far fewer than normal records



in almost every public dataset, so a model can learn to ignore the minority attack classes unless the imbalance is corrected, for example with the ADASYN over-sampling method [4].

A growing number of studies therefore combine three ingredients: a data-balancing step, a feature selection step driven by a metaheuristic optimizer such as the Grey Wolf Optimizer (GWO) [5] or Particle Swarm Optimization (PSO), and a deep learning classifier, often a hybrid Convolutional Neural Network and Long Short-Term Memory (CNN–LSTM) model [6]. Several works go further and hybridise two metaheuristics to search the feature space more effectively [7], [8], while others apply this idea directly to cloud intrusion detection with a classical classifier [9], [10]. However, the design choices, datasets and reported results vary widely across these studies, and it is not always clear where the remaining research gaps lie.

### 1.1 Objective and Contribution of this Review

This paper presents a systematic literature review (SLR) of hybrid optimization-driven machine learning frameworks for intrusion detection, with particular attention to cloud and cloud-adjacent (IoT and IIoT) settings. The specific contributions are: (i) a PRISMA-based search and screening process that selects 30 relevant, peer-reviewed studies; (ii) a thematic organisation of these studies into cloud-specific feature selection work, hybrid metaheuristic optimization work, and optimized deep learning work; (iii) a comparative analysis of the feature selection method, optimizer design, classifier and dataset used in each study, supported by summary charts; and (iv) a set of research gaps that motivate a hybrid GWO–PSO feature selection framework for a CNN–LSTM based cloud IDS, which is the subject of an ongoing dissertation.

The rest of the paper is organised as follows. Section 2 describes the review methodology. Section 3 presents the thematic analysis of the selected studies. Section 4 gives a comparative analysis with a summary table and charts. Section 5 discusses the research gaps, and Section 6 concludes the paper.

## 2. Review Methodology

This review follows the reporting style of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework, adapted to the scale of a dissertation-level literature review.

### 2.1 Research Questions

The review was guided by four research questions (RQ):

1. **RQ1.** Which feature selection strategies, including metaheuristic and hybrid metaheuristic methods, have been used for intrusion detection in cloud, IoT and IIoT environments?
2. **RQ2.** How are these feature selection strategies combined with deep learning classifiers, in particular CNN–LSTM models?
3. **RQ3.** How is class imbalance handled, and how are the resulting models evaluated?
4. **RQ4.** What research gaps remain in combining hybrid dual-optimizer feature selection with CNN–LSTM classifiers for cloud intrusion detection?

### 2.2 Search Strategy

Search strings combining the terms (“cloud” OR “IoT” OR “IIoT”), (“intrusion detection” OR “network security”), and (“Grey Wolf Optimizer” OR “Particle Swarm Optimization” OR “metaheuristic” OR “hybrid optimization” OR “CNN-LSTM” OR “feature selection”) were used. Searches were run mainly through general academic search engines that index Scopus and IEEE-indexed venues (IEEE Access, Scientific Reports, Expert Systems with Applications, and similar sources), and reference lists of retrieved papers were also checked for additional relevant studies (snowballing).

### 2.3 Inclusion and Exclusion Criteria

Table 1 lists the criteria used to decide whether a retrieved paper was kept for the review.



**TABLE 1**
**Inclusion and exclusion criteria**

| Inclusion criteria | Exclusion criteria |
|---|---|
| Published in a peer-reviewed journal or conference with a valid DOI | No DOI could be found, or the record was a preprint, blog post or non-archival source |
| Focuses on intrusion detection, network security or attack classification | Focuses on a topic unrelated to network or system intrusion detection |
| Uses a machine learning or deep learning classifier | Uses only a manual, rule-based, or purely statistical method with no learning component |
| Uses or discusses a metaheuristic optimizer, hybrid optimizer, or a CNN–LSTM style deep model | Uses neither an optimizer nor a deep learning classifier relevant to the review questions |
| Published between 2008 and 2026 (foundational method papers included from any date in this range) | Duplicate of a study already included, or a later preprint of an included published version |

### 2.4 Study Selection Process

Fig. 1 summarises the study selection process using a PRISMA-style flow diagram. Records were identified through the search strategy above, duplicates were removed, titles and abstracts were screened for relevance, and the full text of the remaining records was assessed against the criteria in Table 1. The counts in the figure are based on the searches actually carried out for this review and are given as a representative summary of the screening process rather than a database export.

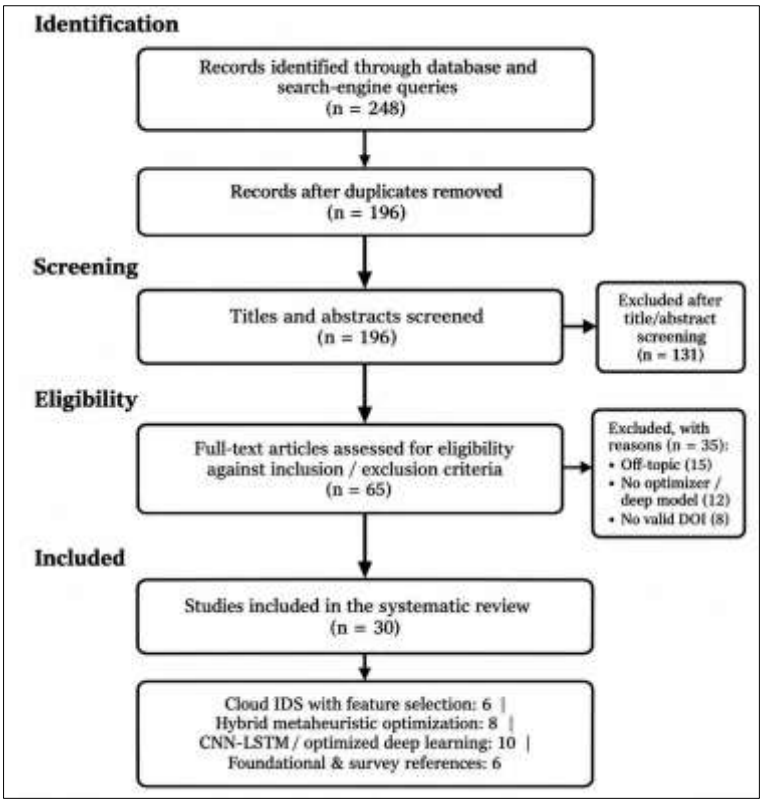



**Fig. 1. PRISMA flow diagram of the study selection process**



### 2.5 Data Extraction and Synthesis

For every included study, the following information was extracted: publication year and venue, target environment (cloud, IoT, IIoT, or general network), feature selection method, whether two optimizers are hybridised, classifier type, data-balancing method, datasets used, and the main reported result. This information forms the basis of the thematic analysis in Section 3 and the comparative tables and charts in Section 4.

## 3. Thematic Analysis of Selected Studies

The 30 included studies are organised into four themes: cloud intrusion detection with feature selection (Section 3.1), hybrid and improved metaheuristic optimization methods (Section 3.2), CNN–LSTM and other optimized deep learning models (Section 3.3), and one representative base framework that combines all three ingredients (Section 3.4).

### 3.1 Cloud Intrusion Detection with Feature Selection

Bakro et al. proposed an improved cloud IDS design that uses a hybrid feature selection approach together with a machine learning classifier [9], and in a later study extended this to a bio-inspired hybrid feature selection method combined with a random forest classifier, reporting accuracy between 92% and 99% across three datasets [10]. Kumar and Kumar applied metaheuristic feature selection to cloud IDS on the CICDDoS2019 and UNSW-NB15 datasets [11]. Farahi et al. proposed a metaheuristic-optimised deep learning framework (built around a module the authors call AQSE) for cloud intrusion detection, evaluated on NSL-KDD, CIC-IDS2017 and UNSW-NB15 with accuracy between 98.65% and 99.69%, though the authors note that their feature search took about 52% longer than a simpler baseline search [12]. Zavvar et al. fused several convolutional neural networks and used GWO to reduce the resulting feature set [13]. Selvakumar et al. proposed a weighted multi-objective GWO for feature selection in network IDS [14], and Abid et al. joined GWO-based feature selection with a CNN-enhanced LightGBM model for IoT threat detection [15].

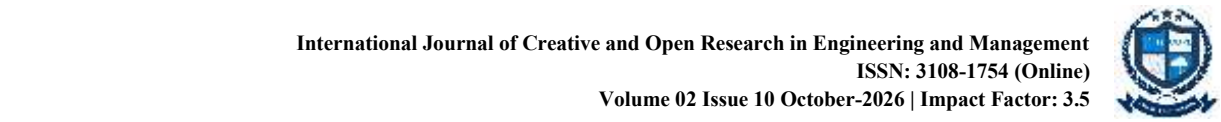
### 3.2 Hybrid and Improved Metaheuristic Optimization Methods

A second group of studies focuses on strengthening the search itself by hybridising two metaheuristics or improving a single one. Alzubi et al. combined a modified binary GWO with PSO for intrusion detection feature selection [7], and Otair et al. proposed a GWO-based PSO for IDS in wireless sensor networks [8]. Alzaqebah et al. modified the basic GWO algorithm to improve its search for IDS [16], while Kareem et al. combined multiple metaheuristic algorithms for feature selection in IoT intrusion detection [17]. Ye et al. proposed an ensemble framework with an improved hybrid breeding optimizer for feature selection, reporting more stable results at the cost of extra computation [18].

More recent studies continue this direction with newer hybrids. Makhadmeh et al. proposed AOAE, a hybrid feature selection approach for IoT networks [19]. Mansouri and Hosseini combined GWO with the Whale Optimization Algorithm (WOA) and added chaos-based search steps before classification with a neural network [20]. Al Abdulwahid et al. proposed an improved binary GWO–PSO hybrid combined with a random forest for large-scale IoT attack detection [21], and Nasir et al. built HED-ID, a metaheuristic-optimised, edge-deployable and explainable IDS [22]. These studies show that hybrid GWO–PSO search has already been explored for IDS, but mostly with classical classifiers such as random forest rather than a CNN–LSTM deep model, and mostly outside a cloud-specific setting.

### 3.3 CNN–LSTM and Optimized Deep Learning Models

A third group of studies focuses on the classifier rather than the feature search. Halbouni et al. showed that a hybrid CNN–LSTM architecture performs well for network intrusion detection [6]. Deore and Bhosale applied hybrid optimisation to build a more robust CNN–LSTM detector [23]. Lilhore et al. proposed an optimised CNN–LSTM with transfer learning for Industry 4.0 networks [24], and Nazir et al. designed a hybrid CNN–LSTM architecture for threat detection in IoT systems [25]. Bahaa et al. proposed a hybrid-optimisation-enabled CNN for IoT intrusion detection [26], and Pramilarani and Kumari used a cost-based random forest classifier for IoT IDS as an alternative to deep learning [27]. Othman et al. combined GWO-based feature selection, SMOTE-based balancing and a CNN–LSTM classifier, reporting 99.68% accuracy on the ToN_IoT dataset [28] and 92.05% on UNSW-NB15, while noting limitations such as single-run results and the use of the test split during feature selection [29].



### 3.4 A Representative Base Framework

Among the reviewed studies, the framework proposed by Chen and Feng [30] is a useful representative example because it combines all three ingredients discussed above: class balancing, feature selection, and a deep learning classifier. As shown in Fig. 2, the framework first applies ADASYN [4] to balance the training data, then uses Recursive Feature Elimination (RFE) with a random forest to select 7 to 10 features depending on the dataset, and finally trains a two-layer 1D-CNN followed by a 140-unit LSTM layer and a softmax output. The reported accuracy is between about 97% and 99% across several public datasets. The authors themselves note that the complex model gives only a small accuracy gain over simpler alternatives while needing considerably more computation, and they list explainability methods such as SHAP or LIME, and improved feature selection, as future work. This combination of strengths and limitations is broadly typical of the wider set of studies reviewed in Sections 3.1 to 3.3, which is why it is used here to illustrate the generalised methodology diagram.

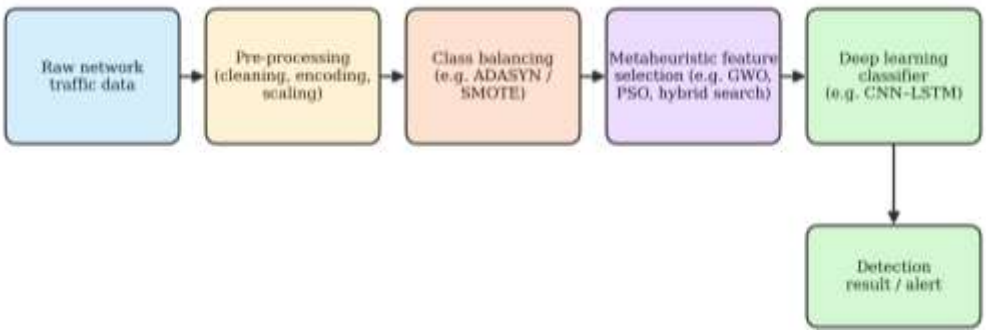



**Fig. 2. Generalised methodology synthesised from the reviewed studies**

## 4. Comparative Analysis

### 4.1 Comparison of Feature Selection and Model Design

Table 2 compares the feature selection method, whether two optimizers are hybridised, the classifier type, the data-balancing method, and the target environment for the studies discussed in Section 3. A dash (–) indicates that the corresponding detail was not clearly reported in the parts of the paper reviewed.

**TABLE 2**
**Comparison of feature selection and model design across selected studies**

| Study | Feature selection method | Two optimizers joined? | Classifier | Data balancing | Environment |
|---|---|---|---|---|---|
| [30] | RFE (not a metaheuristic) | No | CNN–LSTM | ADASYN | IIoT / cloud |
| [9] | Hybrid feature selection | – | Classical ML | – | Cloud |
| [10] | Hybrid bio-inspired | – | Random forest | Yes | Cloud |
| [11] | Metaheuristic | – | – | – | Cloud |
| [12] | Own method (AQSE) | – | QDST-Net | – | Cloud |
| [13] | GWO | No | Fused CNNs | – | – |
| [14] | Multi-objective GWO | No | – | – | Network IDS |
| [15] | GWO | No | CNN + LightGBM | – | IoT |
| [7] | Modified binary GWO | Yes | – | – | Network IDS |



| | | | | | |
|---|---|---|---|---|---|
| | + PSO | | | | |
| [8] | GWO-based PSO | Yes | – | – | Wireless sensor network |
| [16] | Modified GWO | No | – | – | Network IDS |
| [17] | Hybrid metaheuristics | Yes | – | – | IoT |
| [18] | Improved hybrid breeding optimizer | – | Ensemble model | – | – |
| [19] | AOAE hybrid | Yes | – | – | IoT |
| [20] | GWO–WOA with chaos | Yes | Neural network | – | – |
| [21] | Improved binary GWO–PSO | Yes | Random forest | – | IoT |
| [22] | Metaheuristic (explainable) | – | – | – | Edge devices |
| [6] | – (no dedicated FS) | – | CNN–LSTM | – | Network IDS |
| [23] | Hybrid optimisation (model tuning) | – | CNN–LSTM | – | Network IDS |
| [24] | – (transfer learning) | – | CNN–LSTM | – | Industry 4.0 |
| [25] | – (hybrid architecture) | – | CNN–LSTM | – | IoT |
| [26] | Hybrid optimisation (model tuning) | – | CNN | – | IoT |
| [27] | – | – | Random forest (cost-based) | – | IoT |
| [29] | GWO | No | CNN–LSTM | SMOTE | IoT |
| **Proposed direction** | **Hybrid GWO–PSO** | **Yes** | **CNN–LSTM** | **ADASYN** | **Cloud** |

Reading down Table 2, two patterns stand out. First, most studies that hybridise two optimizers pair the result with a classical classifier such as random forest [20], [21] rather than a CNN–LSTM model. Second, most studies that use a CNN–LSTM classifier either skip a dedicated metaheuristic feature selection step [6], [24], [25] or use only a single optimizer [29]. The last row of the table marks the combination, a hybrid GWO–PSO search paired with a CNN–LSTM classifier for cloud traffic, that is not covered by any of the reviewed studies.

### 4.2 Publication Trend

Fig. 3 shows the distribution of the 30 selected studies by publication year. The number of relevant studies has grown steadily since 2022, with more than half of the included studies published in 2025 or 2026, showing that hybrid optimization-driven intrusion detection is an active and growing research area.

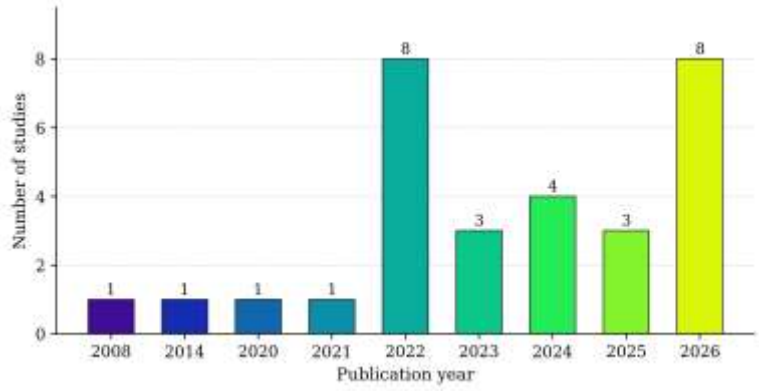



**Fig. 3. Number of selected studies by publication year**

### 4.3 Distribution by Optimization Approach

Fig. 4 groups the 24 studies that propose a specific optimization or feature selection strategy (excluding the six foundational and survey references) into four categories: use of a single metaheuristic for feature selection, a hybrid of two metaheuristics for feature selection, a non-metaheuristic feature selection method such as RFE, and studies that focus mainly on the deep learning classifier without a dedicated feature selection stage. The grouping is based on the authors' description of the main method in each paper and is intended to show the broad balance of the literature rather than an exact count.

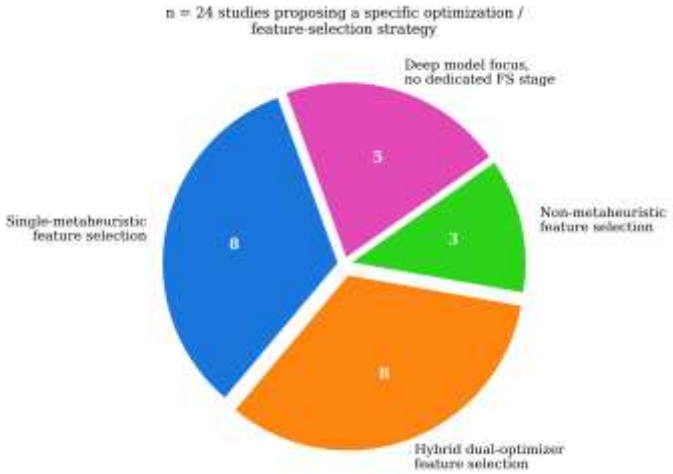



**Fig. 4. Distribution of the reviewed studies by optimization approach**

Single-metaheuristic feature selection and hybrid dual-optimizer feature selection appear in a roughly similar number of studies, which confirms that hybridisation is a well-established idea in this area. However, as Table 2 shows, the hybrid approach is rarely paired with a CNN–LSTM classifier, which is the specific combination targeted by the planned dissertation work.

## 5. Research Gaps

Based on the thematic review in Section 3 and the comparative analysis in Section 4, the following research gaps are identified. Table 3 links each gap to the research question it addresses.

**Gap 1: Hybrid dual-optimizer search is rarely paired with a CNN–LSTM classifier.** Hybrid GWO–PSO and similar dual-optimizer searches have been proposed for IDS [7], [8], [20], [21], but in the studies reviewed here they are almost always combined with a classical classifier such as random forest, not a CNN–LSTM model.

**Gap 2: Cloud-specific evaluation is limited.** Several hybrid optimization studies are evaluated on general network or IoT datasets [7], [8], [17] rather than on datasets that reflect cloud traffic, and the cloud-focused studies that do exist mostly use classical classifiers [9], [10] rather than deep learning.



**Gap 3: Search and training cost is inconsistently reported.** Only some studies report the extra time taken by the optimization step [12], [18], even though this cost is important for practical deployment, and the base framework itself notes a high computation cost for only a small accuracy gain [30].

**Gap 4: Testing practices vary in rigour.** Some studies report results from a single run or use the test split during feature selection [29], which can make reported accuracy look better than it would be in a fair, repeated evaluation.

**Gap 5: Explainability is largely missing.** Only a small number of studies build explainability into the IDS itself [22], and the base framework explicitly lists this as future work [30], even though understanding why a model raises an alert is important for security analysts.

**TABLE 3**
**Research gaps and the research question they relate to**

| Gap | Description | Related RQ |
|---|---|---|
| Gap 1 | Hybrid dual-optimizer feature selection is rarely combined with a CNN–LSTM classifier | RQ1, RQ2 |
| Gap 2 | Hybrid optimization studies are rarely evaluated specifically on cloud traffic | RQ1, RQ2 |
| Gap 3 | Search and training time overhead is inconsistently reported | RQ3 |
| Gap 4 | Single-run results and possible test-split leakage reduce confidence in reported accuracy | RQ3 |
| Gap 5 | Few studies explain the decisions of the trained model | RQ4 |

These gaps together motivate a framework that applies a hybrid GWO–PSO feature selection method to a CNN–LSTM classifier for cloud intrusion detection, with a balanced evaluation protocol and an optional explainability step. This framework forms the basis of the associated M.Tech dissertation.

## 6. Conclusion

This paper has presented a systematic literature review of hybrid optimization-driven machine learning frameworks for intrusion detection, focused on cloud and cloud-adjacent environments. Following a PRISMA-based selection process, 30 studies published between 2008 and 2026 were analysed and organised into cloud-specific feature selection work, hybrid metaheuristic optimization work, and optimized CNN–LSTM based deep learning work. The comparative analysis shows that while metaheuristic feature selection, dual-optimizer hybrids, and CNN–LSTM classifiers are all individually well studied, very few reviewed studies combine a hybrid GWO–PSO style search directly with a CNN–LSTM classifier for cloud network traffic, and reporting of search overhead, repeated-run evaluation, and explainability remains limited. These gaps define a clear and achievable direction for further research and are being taken forward in an ongoing M.Tech dissertation on hybrid optimization-driven intrusion detection for cloud environments.

## References

[1] A. Thakkar and R. Lohiya, “A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions,” *Artificial Intelligence Review*, vol. 55, no. 1, pp. 453–563, 2022, doi: 10.1007/s10462-021-10037-9.

[2] L. Yi, M. Yin, and M. Darbandi, “A deep and systematic review of the intrusion detection systems in the fog environment,” *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 1, Art. no. e4632, 2023, doi: 10.1002/ett.4632.

[3] J. Pacheco, V. H. Benitez, L. C. Felix-Herran, and P. Satam, “Artificial Neural Networks-Based Intrusion Detection System for Internet of Things Fog Nodes,” *IEEE Access*, vol. 8, pp. 73907–73918, 2020, doi: 10.1109/ACCESS.2020.2988055.



[4] H. He, Y. Bai, E. A. Garcia, and S. Li, "ADASYN: Adaptive synthetic sampling approach for imbalanced learning," in *Proc. 2008 IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence)*, 2008, pp. 1322–1328, doi: 10.1109/IJCNN.2008.4633969.

[5] S. Mirjalili, S. M. Mirjalili, and A. Lewis, "Grey Wolf Optimizer," *Advances in Engineering Software*, vol. 69, pp. 46–61, 2014, doi: 10.1016/j.advengsoft.2013.12.007.

[6] A. Halbouni, T. S. Gunawan, M. H. Habaebi, M. Halbouni, M. Kartiwi, and R. Ahmad, "CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System," *IEEE Access*, vol. 10, pp. 99837–99849, 2022, doi: 10.1109/ACCESS.2022.3206425.

[7] Q. M. Alzubi, M. Anbar, Y. Sanjalawe, M. A. Al-Betar, and R. Abdullah, "Intrusion detection system based on hybridizing a modified binary grey wolf optimization and particle swarm optimization," *Expert Systems with Applications*, vol. 204, Art. no. 117597, 2022, doi: 10.1016/j.eswa.2022.117597.

[8] M. Otair, O. T. Ibrahim, L. Abualigah, M. Altalhi, and P. Sumari, "An enhanced Grey Wolf Optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks," *Wireless Networks*, vol. 28, no. 2, pp. 721–744, 2022, doi: 10.1007/s11276-021-02866-x.

[9] M. Bakro et al., "An Improved Design for a Cloud Intrusion Detection System Using Hybrid Features Selection Approach With ML Classifier," *IEEE Access*, vol. 11, pp. 64228–64247, 2023, doi: 10.1109/ACCESS.2023.3289405.

[10] M. Bakro et al., "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along With Random Forest Model," *IEEE Access*, vol. 12, pp. 8846–8874, 2024, doi: 10.1109/ACCESS.2024.3353055.

[11] A. Kumar and S. Kumar, "Metaheuristic-Enhanced Feature Selection for High-Accuracy Intrusion Detection in Cloud Computing," *Procedia Computer Science*, vol. 259, pp. 640–649, 2025, doi: 10.1016/j.procs.2025.04.014.

[12] R. Farahi et al., "Metaheuristic optimized deep learning for intelligent intrusion detection in cloud environments," *Discover Internet of Things*, vol. 6, Art. no. 139, 2026, doi: 10.1007/s43926-026-00485-6.

[13] M. Zavvar et al., "A hybrid intrusion detection method based on multi-convolutional neural networks fusion and grey wolf optimizer," *Journal of Cloud Computing*, vol. 15, Art. no. 77, 2026, doi: 10.1186/s13677-026-00866-w.

[14] B. Selvakumar et al., "Feature selection using feature fusion based weighted multi objective Grey Wolf Optimization for network intrusion detection system," *Cluster Computing*, vol. 28, Art. no. 907, 2025, doi: 10.1007/s10586-025-05608-2.

[15] T. Abid et al., "A novel IoT threat detection using GWO feature selection and CNN-enhanced LightGBM," *Journal of Cloud Computing*, vol. 14, Art. no. 72, 2025, doi: 10.1186/s13677-025-00785-2.

[16] A. Alzaqebah, I. Aljarah, O. Al-Kadi, and R. Damaševičius, "A modified grey wolf optimization algorithm for an intrusion detection system," *Mathematics*, vol. 10, no. 6, Art. no. 999, 2022, doi: 10.3390/math10060999.

[17] S. S. Kareem, R. R. Mostafa, F. A. Hashim, and H. M. El-Bakry, "An effective feature selection model using hybrid metaheuristic algorithms for IoT intrusion detection," *Sensors*, vol. 22, no. 4, Art. no. 1396, 2022, doi: 10.3390/s22041396.

[18] Z. Ye, J. Luo, W. Zhou, M. Wang, and Q. He, "An ensemble framework with improved hybrid breeding optimization-based feature selection for intrusion detection," *Future Generation Computer Systems*, vol. 151, pp. 124–136, 2024, doi: 10.1016/j.future.2023.09.035.

[19] S. N. Makhadmeh, Y. Sanjalawe, M. A. Al-Betar, S. Al-E'mari, S. Fraihat, and E. A. Alzubi, "AOAE: a hybrid feature selection approach for enhanced intrusion detection in internet of things networks," *Neural Computing and Applications*, vol. 38, no. 4, 2026, doi: 10.1007/s00521-025-11763-9.

[20] S. Mansouri and S. Hosseini, "A Chaos-Enhanced Hybrid Metaheuristic Feature Selection for Intrusion Detection Using Artificial Neural Networks," *International Journal of Computational Intelligence Systems*, vol. 19, Art. no. 307, 2026, doi: 10.1007/s44196-026-01417-6.



[21] A. Al Abdulwahid, S. S. Alqahtany, D. Syed, M. S. Al Reshan, K. Rajab, and A. Shaikh, "A hybrid improved binary GWO-PSO with random forest (IBGWO-PSO-RF) based intrusion detection model for large-scale attacks in IoT environment," *Scientific Reports*, vol. 16, Art. no. 3319, 2026, doi: 10.1038/s41598-025-33242-w.

[22] K. Nasir et al., "HED-ID: An edge-deployable and explainable intrusion detection system optimized via metaheuristic learning," *Scientific Reports*, vol. 16, Art. no. 2313, 2026, doi: 10.1038/s41598-025-32183-8.

[23] B. Deore and S. Bhosale, "Hybrid Optimization Enabled Robust CNN-LSTM Technique for Network Intrusion Detection," *IEEE Access*, vol. 10, pp. 65611–65622, 2022, doi: 10.1109/ACCESS.2022.3183213.

[24] U. K. Lilhore et al., "HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning," *Sensors*, vol. 23, no. 18, Art. no. 7856, 2023, doi: 10.3390/s23187856.

[25] A. Nazir et al., "A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem," *Ain Shams Engineering Journal*, vol. 15, Art. no. 102777, 2024, doi: 10.1016/j.asej.2024.102777.

[26] A. Bahaa, A. Sayed, L. Elfangary, and H. Fahmy, "A novel hybrid optimization enabled robust CNN algorithm for an IoT network intrusion detection approach," *PLOS ONE*, vol. 17, no. 12, Art. no. e0278493, 2022, doi: 10.1371/journal.pone.0278493.

[27] K. Pramilarani and P. V. Kumari, "Cost based random forest classifier for intrusion detection system in internet of things," *Applied Soft Computing*, vol. 151, Art. no. 111125, 2024, doi: 10.1016/j.asoc.2023.111125.

[28] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets," *Sustainable Cities and Society*, vol. 72, Art. no. 102994, 2021, doi: 10.1016/j.scs.2021.102994.

[29] A. M. H. Othman, M. F. Ab Razak, A. Firdaus, H. Tahaei, and M. Gheisari, "A Hybrid CNN–LSTM Model for IoT Intrusion Detection: A Robustness Analysis Across Datasets," *Future Internet*, vol. 18, no. 7, Art. no. 345, 2026, doi: 10.3390/fi18070345.

[30] S. Chen and X. Feng, "A novel intrusion detection framework using hybrid deep learning to detect IIoT cloud environments attacks," *Scientific Reports*, vol. 16, Art. no. 11666, 2026, doi: 10.1038/s41598-025-15419-5.