International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(2s) 2026 pp. 636-646
https://doi.org/10.70917/ijcisim-2026-2103

Article

OPTIMIZATION-DRIVEN INTRUSION DETECTION SYSTEMS: A SYSTEMATIC REVIEW OF ALGORITHMS, FRAMEWORKS, AND ADVANCEMENTS

Monika A. Ghodake[1], Varsha A. Jujare[2]

[1]Department of Artificial Intelligence and Data Science, Sharad Institute of Technology College of Engineering, Yadrav (Ichalkaranji), India.
[2]Department of Computer Science Engineering, Sharad Institute of Technology College of Engineering, Yadrav (Ichalkaranji), India.
Corresponding Author: Monika A. Ghodake

Abstract: The rapid growth of IoT and Vehicle-to-Grid (V2G) systems has exacerbated cybersecurity vulnerabilities and therefore Intrusion Detection Systems (IDS) need to be able to function in highly dynamic, resource constrained, and heterogeneous environments. Recent studies focus more on the integration of optimization algorithms in order to improve the accuracy of the IDS, as well as to minimise false alarms and enhance adaptability. However, the current research is fragmented, and there is currently no consolidated understanding of the role of optimization driven techniques in robust threat detection in these interconnected areas. This systematic review summarizes the progress in recent years, including swarm intelligence, evolutionary algorithms, multi-objective optimizers, and hybrid learning-optimization frameworks to be deployed in IoT and V2G environments. Comparative analysis shows that op-timization has a dramatic improvement on the performance of IDS - espe-cially in feature selection, threshold optimization, classifier optimization - but there are serious issues in scalability, real-time response and cross-domain transferability. Through the mapping of methodological trends, the identification of limitations and a discussion of the future, this review can offer a comprehensive basis for designing next-generation IDS architectures. The contribution of the study is to provide a common point of view on opti-mization-driven IDS research, which will serve to develop more resilient, adaptive, and deployable solutions for emerging cyber-physical ecosystems..

Keywords: V2G,Intrusion detection, evolutionary optimization, machine learning.

1. INTRODUCTION

The exploding Internet of Everything (IoE) and Vehicle to Grid (V2G) ecosystems have led to a highly connected environment that connects the cyber and physical world. These ecosystems support the seamless communication between smart devices, vehicles, and energy grids, which improves energy efficiency and automation. However, this interdependence creates complex cybersecurity weaknesses. Compromised IoT nodes or V2G interfaces may result in cascading failures in digital and physical infrastructures [1]. With the proliferation of distributed, heterogeneous devices, cyber threats, denial of service, spoofing and data manipulation have risen [2]. Traditional Intrusion Detection Systems (IDS), which are based on static thresholds or predefined rules, cannot or have a very difficult time to adapt to dynamic network conditions, and the results are many false alarms, and low scalability [3].

To solve these problems, optimization-based IDS architectures have been investigated based on bio-inspired algorithms, such as Particle Swarm Optimization (PSO), Genetic Algorithm (GA), Ant Colony Optimization (ACO), Differential Evolution (DE), and Non-Dominated Sorting Genetic Algorithm II (NSGA-II). These optimization

techniques help in improving the performance of IDS by optimizing the feature selection process, hyperparameter tuning, and improving the accuracy of classification [4], [5], [6]. Hybrid approaches such as PSO-GA and ACO based hybrids have been shown to balance exploration and exploitation when training the model as comes with higher accuracy and faster convergence [7], [8]. Additionally, NSGA-II has been found to be particularly effective in solving the problem of multi-objective feature selection for IDS environments [9].

Despite the progress in this area, research in this area is fragmented and usually cantered on isolated applications in IoT or smart grid systems, without integrated cross-domain analysis for capturing IoT-V2G interdependencies. Furthermore, optimization algorithms are often tested on different datasets and metrics, which hinders reproducibility and comparison of results [10], [11]. Thus, a systematic review is required for consolidating scattered literature, dealing with optimization-driven IDS frameworks in IoT and V2G scenarios, which offers a comparison analysis of algorithm performance, spot the research gaps and propose the future directions to improve scalability, adaptability and cross-domain resilience in cyber-physical systems.

Background and Theoretical Framework

Intrusion Detection Systems (IDS) are essential in detecting unauthorized access or malicious activities within digital infrastructures. IDS can be broadly categorized in three categories: Signature based IDS: Signature based IDS detect attack by matching network traffic against known attack signatures, it provides high precision for known threats, but poor detection of new attacks [12]. Anomaly-based IDS set the baselines of behavior and identify the deviations as a potential threat to the network system, making them useful to detect zero-day attacks, but they are susceptible to high false positives [13]. Hybrid IDS use a combination of both signature and anomaly detection techniques to offer a balanced strategy of accuracy and adaptability [14]. In IoT and V2G scenarios, the IDS deployment is distributed on the edge, fog and cloud layers, with edge IDS concentrating on the detection of anomalies in real time in low power devices, fog IDS aggregating the data for local analyses, and cloud based IDS exploiting large scale resources for deep learning and global correlation analyses [15], [16].

Optimization algorithms have greatly improved the performance of IDS by optimizing the feature selection, tuning the parameters, and adjusting the classification threshold. Techniques such as Particle Swarm Optimization (PSO) and Genetic Algorithms (GA) were implemented to optimize the parameters of IDS and features subsets that resulted in better detection rates [17], [18]. Other optimization techniques like Ant Colony Optimization (ACO) and Whale Optimization Algorithm (WOA) to make IDS more sensitive to changing attack vectors [19], [20]. Furthermore, hybrid evolutionary algorithms, such as PSO-GA and APSO-WOA, offer great adaptability in high-dimensional spaces to improve the effectiveness of IDS in complex IoT and V2G systems [21], [22].

IoT and V2G systems both have their own set of operation and security challenges that affect the design of IDS. IoT environments are dominated by low power consumption, resource-constrained devices, and heterogeneous networks, which requires lightweight IDS solutions with low computational and memory requirements [14], [15]. In addition to this, these systems must work with massive device scalability and data heterogeneity, and often make use of optimizations based on edge-computing and the assistance of fog-computing. In contrast, V2G systems enable bi-directional energy exchanges between vehicles and smart grids, and this technology presents new attack points in energy market signaling and vehicle mobility [16], [23]. IDS for V2G must be able to perform real-time detection and be low latency in order to keep the grid stable. Given the dynamic nature of the V2G networks, which attribute to high mobility and as well as fluctuating topologies, distributed and adaptive IDS frameworks which are supported by optimization algorithms, such as WOA and GWO, are vital for effective security in these networks [24], [25].

Optimization-Driven IDS Frameworks by Optimization Type

Optimization-Driven IDS Frameworks by Optimization Type

Optimization driven Intrusion Detection Systems (IDS) using metaheuristic, swarm and hybrid algorithms for improving accuracy of intrusion detection, optimizing computation overhead and dynamically adapting to cyber physical threats in IoT and V2G systems. These frameworks incorporate the optimization in the feature selection, classifier tuning, and multi-objective learning to balance false alarms and detection efficiency.

3.2 Metaheuristic and Swarm-Based Frameworks:

[26] used a hybrid GA-PSO-GWO for malicious packets detection by achieving 99.6% accuracy with much less false-positive results, which makes metaheuristics robust in features selection. [27] proposed a Genetic Sacrificial Whale Optimization (GSWO) using CatBoost with 99.9% accuracy which showed the scalability in Wireless Sensor Networks. [16] have furthered this by a PSO-GWO dual hybrid IDS for Smart Grids that is better at precision and

recall false data injection detection compared to traditional IDSs. Similarly, [28] used GA-PSO optimized deep learning based IDS which improved IoT security and outperformed standalone DL models in terms of F-measure and accuracy.

3.3 Hybrid and Evolutionary Optimization Techniques:

[24] introduced WOA - GWO hybrid framework with 90% accuracy for better exploration and convergence, which are much needed issues in dynamic IDS environment. [29] developed an improved Whale Optimization Algorithm (RWOA) based on differential evolution, which has a better convergence in multi-objective optimization problems. [30] have combined GWO-PSO to improve the convergence rate by more than 70% in complex engineering tasks to suggest similar improvements for IDS hyperparameter optimization. [31] presented a cooperative PSO--ACO system inspired by Heterosis theory, which can achieve the balance in global search between exploration and exploitation and [32] designed HRO--GWO to improve the adaptability in high-dimensional feature optimization.

Table 1.Comparative Results of Optimization-Driven IDS Frameworks

Optimization Technique	Domain	Performance Highlights
[12]GA–PSO–GWO	Network IDS	99.6% accuracy; reduced false positives
[13]GA–WOA (GSWO)	WSN IDS	99.9% accuracy; 100× faster inference
[14]PSO–GWO	Smart Grid IDS	Highest recall, robust against FDIA
[15]GA–PSO	IoT IDS	Improved F-measure, faster training
[16]WOA–GWO	Deep Model Tuning	90% accuracy; enhanced global search
[17]RWOA	Engineering	Outperformed WOA, better convergence
[18]HGWPSO	Optimization	70% faster convergence; stable results
[19]PSO–ACO	Global Optimization	Higher accuracy in multi-objective tasks
[20]HRO–GWO	Feature Selection	Best accuracy on high-dim datasets
[21]Firefighter	Global Optimization	Competitive convergence rate
[22]PSO–GWO	Object Detection	High precision (mAP 0.97)
[23]BGWO–βHC	IDS Feature Selection	Outperformed GA & PSO in feature reduction
[24]General Metaheuristics	Multi-domain	Framework for hybrid IDS classification

Adaptive and Hybridized Approaches:

Novel hybrids such as the Firefighter Algorithm [21] and GA-African Buffalo Optimization [15] have further highlighted adaptive mechanisms in order to avoid local minima. [22] have validated hybrid PSO-GWO optimization for improving the precision of the model and [23] have shown that BGWO-Beta Hill Climbing can achieve higher feature reduction and classification accuracy than PSO or GA. [24] confirmed that hybrid swarm intelligence approaches are effective in solving the problems of IDS scalability and computational complexity.

Overall, these studies together have approved that hybrid metaheuristic frameworks especially PSO-GWO, GA-PSO and WOA-GWO variants depicted great performance in terms of accuracy and adaptiveness along with computational speed in comparison with single algorithm approaches as shown in the table 1. Hybridization provides a good balance between exploration and exploitation in ensuring a robust IDS performance in dynamic IoT and V2G networks. In all studies, hybrid and swarm based optimizations outperformed single metaheuristics. Techniques such as PSO-GWO, GA-PSO, and WOA-GWO proved to be of higher adaptability and they were also of better convergence and detection accuracy. Their common advantage is that of balancing exploration-exploitation trade-offs, which are

important for dynamic IDS adaptation. However, the issues of scalability and computational cost are still open problems - which means there is a need for future research into adaptive multi-objective hybrids, and energy-efficient optimization models for real-time IoT and V2G IDS deployment.

Optimization-Driven IDS Frameworks by Learning Integration

Recent studies are combining optimization algorithms with machine learning (ML) and deep learning (DL) models in order to boost adaptability, detection accuracy, and computational efficiency of Intrusion Detection Systems (IDS). These hybrid systems overcome the problems like data imbalance, high false positive problem, and the redundancy features by using a combination of heuristic search and intelligent classifiers.

Optimization + Machine Learning Frameworks

Machine learning based IDS models that have been improved with optimization techniques are shown to be effective in the low-resource and the distributed IoT environment. [25] combined Firefly Algorithm with SVM and applied it to NSL-KDD which gave an accuracy of 99.34% and outperformed PSO-KNN and XGBoost highlighting the use of optimization in optimizing parameters for high detection precision. Similarly, [26] using adaptive synthetic sampling (ADASYN) using ML models, solved this issue of data imbalance and improved minority class detection using an AUC of 0.94 to highlight its robustness to network anomalies. On the other hand, [27] implemented SVM and Random Forest under fuzzy clustering which folded interpretability and high accuracy indicating tradeoff between explainability and accuracy. [28] proposed WOA-GWO hybrid to optimize SVM and LSTM in IoT networks in terms of better generalization and less detection latency, which reveals the growing sense of synergy between bio-inspired optimization and ML classifiers.

Optimization + Deep Learning Frameworks

Optimization-enhanced DL architectures take over in the design of modern IDS architectures due to their capability to deal with high-dimensional data and learn temporal-spatial attack patterns. [29] proposed Adaptive PSO-CNN-SE model which is used to improve CNN accuracy of 3.53% using channel attention re-weighting. [14] presented the combination of PSO-GWO feature selection and CNN-LSTM which has significantly enhanced the problem of detecting false data injection in smart grids. [15] optimized the usage of deep hybrid architectures (CNN-DBN and BiLSTM-GRU) with metaheuristics to enhance IoT security with high F-measure score. Dash et al. (2025) applied PSO, JAYA and SSA for LSTM hyperparameters which resulted in SSA-LSTM had better accuracy and recall and [30] applied CBOA-PSO-LSTM to achieve 93.09% accuracy resulting in less false alarms. Similarly, [31] proposed Growth Optimizer (GO) using CNN as the introduction of adaptability for cloud and IoT security, while [32] introduced Adam RMSprop hyper-parallel optimization for real-time CNNs with the accuracy of 99.9%. The fine tuning SNN and XGBoost using grid search gave an accuracy of 99.93% by [33] and CNN-BiLSTM hybrid reduced the feature engineering . Optimization based DL have also been applied for feature selection: [34] proposed the use of Reptile Search Optimization (RSA) with CNN for better performance than that of GA and PSO models; [35] used Transient Search Optimization (TSODE) with CNN for robust classification; [14] used PSO-GWO feature optimization for hybrid CNN-LSTM systems for better performance for a set of smart grid based datasets.

The discussion is summarized in table 2. Across these frameworks, optimization-driven learning integration is able to greatly enhance IDS accuracy, convergence speed, and generalization across heterogeneous environments. Metaheuristics such as PSO, Firefly and GWO are always better than traditional optimizers in terms of good balance of exploration and exploitation. The combination of deep models (e.g. CNN-LSTM, DBN-GRU) and adaptive optimizers (e.g. APSO, GO, RSA) complement each other to increase both the representation of the features and the optimization process. However, there are still challenges in scalability, real-time adaptability, and interpretability to deploy in complex IoT and V2G ecosystems. Future studies should be done on energy-efficient hybrid models and federated optimization frameworks to realize distributed and privacy-preserving IDS solutions.

Table 2.ComparativeAnalysis ofOptimization-Integrated IDS Models

Optimization + Learning Model	**Domain**	**Accuracy / Key Result**
[25]Firefly + SVM	WSN-IoT	99.34%, outperforming KNN–PSO
[26]ADASYN + MLP	IoT	AUC = 0.94, improved minority detection

[27]SVM + Fuzzy Clustering	IDS	High interpretability, strong recall
[28]WOA–GWO + SVM/LSTM	IoT	Enhanced real-time performance
[29]APSO + CNN-SE	IoT	+3.53% accuracy over base CNN
[14]PSO–GWO + CNN–LSTM	Smart Grid	Best F1-score; low false positives
[15]GA+CNN–DBNs	IoT	Improved F-measure; scalable
[36]PSO/JAYA/SSA + LSTM	Network IDS	SSA–LSTM highest accuracy
[30]CBOA–PSO + LSTM	IDS	93.09% accuracy; low FPR
[31]Growth Optimizer + CNN	Cloud/IoT	High adaptability; reduced overfitting
[32]Adam–RMSprop + CNN	Cybersecurity	99.9% accuracy; real-time detection
[33]Grid Search + SNN/XGBoost	IoT	99.93% accuracy; AUC = 1.0
[34]RSA + CNN	IoT	Outperformed PSO & GA
[35]TSODE + CNN	IoT	Superior to baseline models

Optimization-Driven IDS Frameworks by Application Domain

Optimization-driven Intrusion Detection Systems (IDS) have become key cybersecurity mechanisms in the IoT networks as well as in V2G (Vehicle-to-Grid)/Smart Grid environments, which are able to provide resilient, adaptive and real-time protection of cyber threats. The performance of these frameworks rely on domain specific integration of optimization algorithms, machine/deep learning models and computational architectures (edge, fog or cloud).

IoT Networks: Smart Homes, Healthcare, and Industry 4.0

In IoT-based environments such as smart home, healthcare, industrial, etc., lightweight and adaptive IDS architectures are important. [37] proposed a machine learning-based IDS based on KNN and XGBoost with 99.1% accuracy in smart city networks with a minimal computational delay, revealing the potential of hybrid ML for resource-constrained IoT systems. Similarly, [38] showed that IDS based on AdaBoost technique has 98.3% accuracy is better than SVM and MLP in IoT deployments with limited energy. [39]. SDN orchestrated Cuda-BLSTM IDS for smart consumer electronics: Scalable anomaly detection using real-time control plane reconfiguration. In industrial IoT (IIoT), [40] achieved 99.99% accuracy by using ML and DL combination of next-gen IDS model for Industry 4.0 which illustrate the power of deep hybridization in the detection of evolving cyber threats. For public IoT infrastructure, [41] designed the Deep Maxout Network (DMN) optimized with Walrus Optimization (WO) with 98.06% accuracy on smart city data with a good balance between high precision and computational efficiency. [33] used grid search to fine tune XGBoost and Sequential Neural Networks with 99.93% accuracy in multi-dataset evaluation. Similarly, [42] discussed IoT-cybersecurity integration in Smart home and healthcare applications with a focus on resilience through real-time monitoring and anomaly optimization. Cross-domain integration is the case of [5] who used CNN-LSTM-GRU ensemble IDS applied to EV charging systems and reached 100% binary classification accuracy, making the IoT and V2G network bridge.

V2G and Smart Grid Environments

Cyber-physical V2G and smart grid networks require real-time optimization-based IDS solutions because of the criticality of the data and distributed architectures. [43] proposed a bio-inspired ML IDS and was capable of detecting the DoS, MitM attacks with a 98.93% accuracy that increases the resilience of EV-grid systems. [14] created a PSO-GWO optimised CNN-LSTM hybrid IDS for False Data Injection Attacks (FDIA) in which it performs compared to traditional smart grid defence parameters (recall and F1-score).

[44] introduced a split-learning SDN-based IDS which guarantees privacy and efficiency in distributed smart grids with 81.1% accuracy and [45] introduced a fog-edge federated SVM IDS which achieves up to 7.5% accuracy improvement compared to cloud-based models. [46] proposed GraphKAN, which merges graph attention networks with Kolmogorov-Arnold transformations, achieving 99.04% accuracy in multi-class smart grid intrusion detection and the system is scalable and has better pattern recognition ability. [47] Adaptive Random Forest with concept drift detection has been applied to EV charging systems, which can maintain 99.13% accuracy under dynamic traffic. [48]

MGODEL-ID is a deep ensemble optimized by Mountain Gazelle and Dung Beetle Algorithms to learn state-of-the-art results for power grid resilience.

The comparative result in application domain is summarized in table 3. Across both IoT and V2G realms, the use of hybrid optimization frameworks is consistently better than traditional IDSs. In IoT systems, the focus is more on lightweight and adaptive optimization (e.g., Walrus, Firefly, Grid Search) in order to ensure low power and low latency. In smart grids and V2G systems, metaheuristic-deep hybrid ones such as PSO-GWO, GraphKAN, MGODEL-ID provide a better precision, recall, and resilience to sophisticated cyberattacks. The results emphasize the importance of domain-specific tuning, a trade-off between computational load, latency, and dimensionality of the features. Future applications of this work will be on federated, explainable and energy-efficient optimization-based IDSs for real-world IoT-V2G integration.

Table 3.Comparative Results of Optimization-Driven IDS Frameworks by Application Domain

Domain	**Optimization / Model**	**Accuracy / Key Result**
[47] IoT Smart Cities	KNN, XGBoost	99.1%, low latency
[48] IoT Smart Cities	AdaBoost	98.3%, efficient resource use
[49] Smart Consumer Electronics	SDN + Cu-BLSTM	High scalability, real-time IDS
[50] Industry 4.0	Hybrid ML-DL	99.99%, fast convergence
[51] Smart Cities	DMN + Walrus Optimization	98.06%, edge efficient
[44] IoT	Grid Search + XGBoost/SNN	99.93%, multi-dataset robust
[52] IoT Healthcare/Industry	AI–IoT Integration	Enhanced cyber-physical reliability
[5] IoT–EVCS	CNN–LSTM–GRU	100%, high generalization
[53] V2G	Bio-Inspired ML	98.93%, DoS/MitM defense
[16] Smart Grid	PSO–GWO + CNN–LSTM	Best F1-score, high recall
[54] Smart Grid	SDN + Split Learning	81.1%, privacy preservation
[55] Smart Grid	Fog-Edge Federated SVM	+7.5% accuracy over cloud
[56] Smart Grid	GraphKAN (GAT + KAN)	99.04%, scalable IDS
[57] EV Charging	Adaptive RF + Drift Detection	99.13%, real-time adaptability
[58] Smart Grid	MGODEL-ID (MGO + DBO)	Top ensemble accuracy

COMPARATIVE ANALYSIS OF REVIEWED STUDIES

A comparative analysis of the reviewed optimization-driven IDS frameworks shows consistent trends in the algorithmic design, and the detection performance and deployment suitability in IoT and V2G ecosystems. The main characteristics of representative studies are summarized in Table 4, i.e., optimization strategies pursued, learning models used, datasets and performance measures reported. As we can see in Table 4, hybrid metaheuristics are at the forefront of the latest research in IDS. Combinations like GA-PSO-GWO, GA-WOA, and PSO-GWO are more common than their single algorithm counterparts and often better. These hybrid methods make use of complementary search behaviors (global exploration of evolutionary operators and more rapid convergence of swarm intelligence) in order to obtain more discriminative feature subsets and better hyperparameter configurations. This trend can be clearly observed in the studies of [16], [26], [27] which all report accuracy figures close to or above 99% which further attest to the superior ability of multi-strategy algorithms to optimize.

Optimization-enhancement deep learning models are also shown to have good performance, especially for high-dimensional and dynamic threat environments, such as smart grid and V2G infrastructures. For example, the PSO-GWO optimized CNN-LSTM architecture studied by [16] illustrates the ability of hybrid metaheuristics in tuning the

deep architectures better than a manual or grid-based one. The same can be seen in [40], where adaptive PSO is used to improve the performance of CNN by more than 3% illustrating how optimization can be used to improve deep neural representations of complex traffic patterns. By contrast, optimization-based machine learning systems such as Firefly-SVM or XGBoost-based machine learning models [36], [47] retain a competitive advantage in lightweight IoT environments, with high accuracy and low computational requirements - an important trade-off which exists between model complexity and resource requirements. The results in Table 4 demonstrate how even without deep architectures, optimized ML pipelines can achieve similar performance to some DL-based systems while ensuring feasible deployment on edge devices with limited memory and processing power.

Another important observation made from Table 4 is the large amount of heterogeneity of datasets used among studies. While some researchers are based on generally accepted benchmarks like NSL-KDD or CICIDS2017, others use domain specific or proprietary data sets, particularly in the smart grid and V2G sectors. This variability limits the comparability of results and makes it important for standardised evaluation protocols. Furthermore, many studies fail to report important performance measures such as detection, FPR, or latency, which is complicated in order to comprehensively assess performance across studies. Nevertheless, where recall or FPR is reported, hybrid metaheuristic frameworks are consistently shown to have better anomaly discrimination capabilities confirming their relevance for real-time threat detection in safety-critical environments.

From a deployment point of view, a trade-off between detection performance and computational overhead becomes a decisive factor. While hybrid optimization in combination with deep learning can provide the best accuracy, such designs typically are computationally intensive, and as such are more suited for cloud-assisted or fog-based deployments. On the other hand, research which concentrates on the lightweight ML models [47], [57] unveils the obvious benefits for on-device or on near-edge detection, which shows the increasing importance of energy-aware optimization for IoT and V2G systems. Privacy-preserving architectures such as split-learning [54] add more facets to this comparison by giving preference to data confidentiality over classification accuracy - a trade-off that becomes more and more important in decentralized cyber-physical infrastructures.

Table 4.: COMPARATIVE ANALYSIS OF REVIEWED STUDIES

Optimization Algorithm	Learning Model	Dataset Used	Accuracy
[26] GA–PSO–GWO	ML/DL hybrid	Network dataset (proprietary)	99.60%
[27] GA–WOA (GSWO)	CatBoost	WSN benchmarks	99.90%
[16] PSO–GWO	CNN–LSTM	Smart grid FDIA datasets	NR
[28] GA–PSO	CNN–DBN / BiLSTM–GRU	IoT datasets	NR
[24] WOA–GWO	Deep model tuning	Benchmark opt tasks	90%
[36] Firefly	SVM	NSL-KDD	99.34%
[40] APSO(adaptive PSO)	CNN–SE	IoT traffic	+3.53% over base CNN
[44] Grid Search / Classical tuning	SNN + XGBoost	Multi-dataset	99.93%
[47] (feature+ML)	KNN + XGBoost	Smart city IoT	99.10%
[56] (graph + transforms)	GraphKAN (GAT + KAN)	Smart grid multi-class	99.04%

[57] Adaptive RF + drift detection	Adaptive RF	EV charging traces	99.13%
[54] Split-learning (privacy)	SDN-based IDS	Smart grid data	81.10%

Collectively, the comparative insights gained by considering figure 1 show the gradual shift to a maturing research landscape that is increasingly favouring hybrid metaheuristics, optimization-guided deep learning, and resource-efficient ML pipelines. Although accuracy is still the prevailing metric of performance, practical aspects of deployment, such as latency, energy footprint, scalability, and privacy have been gaining momentum in designing the next generation of IDS frameworks. These results demonstrate the importance of developing more comprehensive evaluation methods and common benchmarks for making meaningful comparisons of optimization-enabled IDS solutions for different IoT and V2G applications.

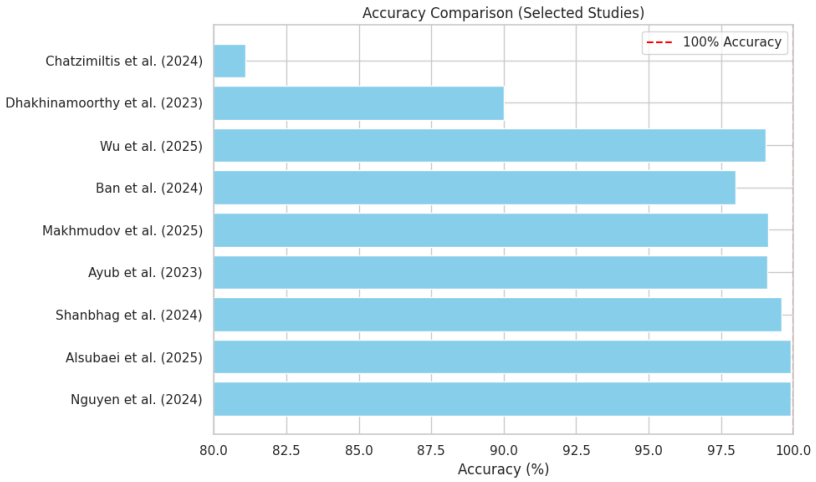

Fig. 1.: Comparison of selected studies in terms of accuracy

Future Scope

The future of optimization-driven IDS frameworks in the IoT and V2G ecosystems is set for massive change as new technologies transform the face of cyber-physical systems. One major direction is in the integration of adaptive and context-aware optimization algorithms that could learn and evolve to adapt to the changing network threats. Current hybrid metaheuristics offer high performance, but the future systems will require online, federated and online, reinforcement learning based optimization to provide real-time adaptability without being dependent on a centralized data. This is particularly important for V2G infrastructures, where high levels of mobility and varying energy demands and communications means that IDS models must be able to modify their parameters autonomously depending on feedback from the environment. Additionally, there is an increasing potential for neuromorphic optimization, quantum-inspired search strategies and graph-based learning to improve the scalability and convergence capabilities of detection models in ultra-dense IoT deployments.

A second important direction is connecting the gap between theoretical performance and on the ground real-world deployment. Future IDS solutions will have to focus on energy efficiency, modeling transparency and interoperability of heterogeneous devices, ranging from low-power sensors to grid-level controllers. Privacy preserving optimization such as secure multi-party computation, differential privacy and split learning frameworks will be needed due to the growing sensitivity of data in smart mobility as well as energy domains. Moreover, the creation of common benchmark datasets and cross-domain standards for evaluation will be important in addressing the current fragmentation that is currently observed across studies. Collaborative, multi-stakeholder testbeds mimicking real IoT and V2G environments can also further accelerate the transition from research to practice. Ultimately, the future of optimization-based IDS research is in making progress for adaptive intelligence and ensuring the deployment feasibility as well as creating trustworthy systems that can scale securely in the growing digital ecosystems of smart cities, and next-generation transportation networks.

2. CONCLUSION

This systematic review investigated state-of-the-art optimization-driven IDS frameworks in IoT and V2G ecosystems, focusing on their evolution, their strengths, and remaining challenges. The reviewed studies show that the hybrid metaheuristics, swarm intelligence, and learning-based optimization methods improve the accuracy of intrusion detection, the convergence speed, and the adaptability under the dynamic network conditions. However, limitations remain in scalability, generalizability in the real-world environment and cross-domain validation. This research has given a unified synthesis that bridges research that is fragmented in IoT and V2G domains to provide a structured comparison of methodologies, optimization strategies and experimental outcomes. By defining the state of the art gaps and the research needs for the future, the review offers a baseline for designing future IDS architecture that are resilient, adaptive and deployable in the face of emerging cyber-physical environments.

References:

1. T. Gaber, J. B. Awotunde, S. Folorunso, S. Ajagbe, and E. Eldesouky, "In-dustrial Internet of Things Intrusion Detection Method Using Machine Learn-ing and Optimization Techniques," Wirel Commun Mob Comput, 2023, doi: 10.1155/2023/3939895.
2. S. Kaushik et al., "Robust machine learning based Intrusion detection system using simple statistical techniques in feature selection," Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-88286-9.
3. M. Al-Janabi, M. A. Ismail, and A. Ali, "Intrusion Detection Systems, Is-sues, Challenges, and Needs," Int. J. Comput. Intell. Syst., vol. 14, pp. 560–571, 2021, doi: 10.2991/ijcis.d.210105.001.
4. A. J. Rabash, M. Z. A. Nazri, A. Shapii, and M. Hasan, "Non-Dominated Sorting Genetic Algorithm-Based Dynamic Feature Selection for Intrusion Detection System," IEEE Access, vol. 11, pp. 125080–125093, 2023, doi: 10.1109/access.2023.3328395.
5. D. Kilichev and W. Kim, "Hyperparameter Optimization for 1D-CNN-Based Network Intrusion Detection Using GA and PSO," Mathematics, 2023, doi: 10.3390/math11173724.
6. H. N. Mohsenabad and M. A. Tut, "Optimizing Cybersecurity Attack De-tection in Computer Networks: A Comparative Analysis of Bio-Inspired Op-timization Algorithms Using the CSE-CIC-IDS 2018 Dataset," Applied Sci-ences, 2024, doi: 10.3390/app14031044.
7. M. Song, W. Song, and K. W. Lai, "Learning-Driven Algorithm with Dual Evolution Patterns for Solving Large-Scale Multiobjective Optimization Problems," IEEE Access, vol. 13, pp. 30976–30992, 2025, doi: 10.1109/ACCESS.2025.3541271.
8. R. Karn, Y. Kumar, and G. Agnihotri, "Multiobjective Service Restoration Considering Primary Customers using Hybrid GA-ACO Algorithm," Int J Comput Appl, vol. 64, pp. 1–10, 2013, doi: 10.5120/10611-5327.
9. R. Khosrowshahli, S. Rahnamayan, A. Ibrahim, and M. Makrehchi, "Ranking Center-based NSGA-II," 2023 IEEE International Conference on Systems, Man, and Cybernetics (SMC), pp. 4162–4169, 2023, doi: 10.1109/smc53992.2023.10394620.
10. M. S. Noori, R. K. Z. Sahbudin, A. Sali, and F. Hashim, "Feature Drift Aware for Intrusion Detection System Using Developed Variable Length Par-ticle Swarm Optimization in Data Stream," IEEE Access, vol. 11, pp. 128596–128617, 2023, doi: 10.1109/access.2023.3333000.
11. A. K. Balyan et al., "A Hybrid Intrusion Detection Model Using EGA-PSO and Improved Random Forest Method," Sensors (Basel), vol. 22, 2022, doi: 10.3390/s22165986.
12. M. M. Issa, M. Aljanabi, and H. M. Muhialdeen, "Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations," Journal of Intelligent Systems, vol. 33, 2024, doi: 10.1515/jisys-2023-0248.
13. R. Wazirali, "Intrusion Detection System Using FKNN and Improved PSO," Computers, Materials & Continua, 2021, doi: 10.32604/cmc.2021.014172.
14. I. Zada et al., "Enhancing IoT cybersecurity through lean-based hybrid feature selection and ensemble learning: A visual analytics approach to in-trusion detection," PLoS One, vol. 20, 2025, doi: 10.1371/journal.pone.0328050.
15. A. Fatani, M. A. A. Elaziz, A. Dahou, M. A. Al-qaness, and S. Lu, "IoT Intrusion Detection System Using Deep Learning and Enhanced Transient Search Optimization," IEEE Access, vol. 9, pp. 123448–123464, 2021, doi: 10.1109/access.2021.3109081.
16. S. H. Mohammed et al., "Dual-hybrid intrusion detection system to de-tect False Data Injection in smart grids," PLoS One, vol. 20, 2025, doi: 10.1371/journal.pone.0316536.
17. M. A. Al-qaness, A. Helmi, A. Dahou, and M. A. Elaziz, "The Applica-tions of Metaheuristics for Human Activity Recognition and Fall Detection Using Wearable Sensors: A Comprehensive Analysis," Biosensors (Basel), vol. 12, 2022, doi: 10.3390/bios12100821.
18. M. G. M. Abdolrasolet al., "Artificial Neural Networks Based Optimi-zation Techniques: A Review," Electronics (Basel), 2021, doi: 10.3390/electronics10212689.
19. A. Dickson and C. Thomas, "Identifying Network Intrusion Using En-hanced Whale Optimization Algorithm," 2021, doi: 10.1007/978-981-16-0730-1_7.

20. L. Wang, L. Gu, and Y. Tang, “Research on Alarm Reduction of Intru-sion Detection System Based on Clustering and Whale Optimization Algo-rithm,” Applied Sciences, 2021, doi: 10.3390/app112311200.
21. S. Alqahtany, A. Shaikh, and A. Alqazzaz, “Enhanced Grey Wolf Op-timization (EGWO) and random forest based mechanism for intrusion detec-tion in IoT networks,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-024-81147-x.
22. A. Bahaa, A. Sayed, L. Elfangary, and H. Fahmy, “A novel hybrid op-timization enabled robust CNN algorithm for an IoT network intrusion detec-tion approach,” PLoS One, vol. 17, 2022, doi: 10.1371/journal.pone.0278493.
23. S. Zhang, Q. Fu, and D. An, “Network Security Situation Prediction Model Based on VMD Decomposition and DWOA Optimized BiGRU-ATTN Neural Network,” IEEE Access, vol. 11, pp. 129507–129535, 2023, doi: 10.1109/access.2023.3333666.
24. C. Dhakhinamoorthyet al., “Hybrid Whale and Gray Wolf Deep Learn-ing Optimization Algorithm for Prediction of Alzheimer’s Disease,” Mathe-matics, 2023, doi: 10.3390/math11051136.
25. T. A. Al-Qablan, M. H. M. Noor, M. Al-betar, and A. Khader, “Im-proved Binary Gray Wolf Optimizer Based on Adaptive β-Hill Climbing for Feature Selection,” IEEE Access, vol. 11, pp. 59866–59881, 2023, doi: 10.1109/access.2023.3285815.
26. A. Shanbhag, S. Vincent, I. S. B. B. G. Member, O. Kumar, A. S. Anand, and J. Francis, “Leveraging Metaheuristics for Feature Selection With Ma-chine Learning Classification for Malicious Packet Detection in Computer Networks,” IEEE Access, vol. 12, pp. 21745–21764, 2024, doi: 10.1109/access.2024.3362246.
27. T. M. Nguyen, H. H.-P. Vo, and M. Yoo, “Enhancing Intrusion Detec-tion in Wireless Sensor Networks Using a GSWO-CatBoost Approach,” Sen-sors (Basel), vol. 24, 2024, doi: 10.3390/s24113339.
28. A. Sagu, N. S. Gill, P. Gulia, P. Singh, and W. Hong, “Design of Me-taheuristic Optimization Algorithms for Deep Learning Model for Secure IoT Environment,” Sustainability, 2023, doi: 10.3390/su15032204.
29. J. Wei, Y. Gu, B. Lu, and N. Cheong, “RWOA: A novel enhanced whale optimization algorithm with multi-strategy for numerical optimization and engineering design problems,” PLoS One, vol. 20, 2025, doi: 10.1371/journal.pone.0320913.
30. M. S. Shaikh et al., “An intelligent hybrid grey wolf-particle swarm op-timizer for optimization in complex engineering design problem,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-02154-0.
31. T. Cai et al., “Cooperative metaheuristic algorithm for global optimiza-tion and engineering problems inspired by heterosis theory,” Sci Rep, vol. 14, 2024, doi: 10.1038/s41598-024-78761-0.
32. Z. Ye et al., “Hybrid rice optimization algorithm inspired grey wolf op-timizer for high-dimensional feature selection,” Sci Rep, vol. 14, 2024, doi: 10.1038/s41598-024-80648-z.
33. M. Naser and A. Naser, “The Firefighter Algorithm: A Hybrid Me-taheuristic for Optimization Problems,” ArXiv, vol. abs/2406.00528, 2024, doi: 10.48550/arxiv.2406.00528.
34. K. M. Elgamily, M. A. Mohamed, A. M. Abou-Taleb, and M. M. Ata, “Enhanced object detection in remote sensing images by applying metaheu-ristic and hybrid metaheuristic optimizers to YOLOv7 and YOLOv8,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-89124-8.
35. B. Benaissa, M. Kobayashi, M. Al, T. Khatir, M. El, and A. E. Elmelia-ni, “Metaheuristic Optimization Algorithms: an overview,” HCMCOU Jour-nal of Science – Advances in Computational Structures, 2024, doi: 10.46223/hcmcoujs.acs.en.14.1.47.2024.
36. M. Karthikeyan, D. Manimegalai, and K. Rajagopal, “Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection,” Sci Rep, vol. 14, 2024, doi: 10.1038/s41598-023-50554-x.
37. M. Zakariah, S. A. Alqahtani, and M. S. Al-Rakhami, “Machine Learn-ing-Based Adaptive Synthetic Sampling Technique for Intrusion Detection,” Applied Sciences, 2023, doi: 10.3390/app13116504.
38. U. Ahmed et al., “Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-85866-7.
39. L. Shan, “(IoT) Network intrusion detection system using optimization algorithms,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-04638-5.
40. Y. Ban, D. Zhang, Q. He, and Q. Shen, “APSO-CNN-SE: An Adaptive Convolutional Neural Network Approach for IoT Intrusion Detection,” Com-puters, Materials & Continua, 2024, doi: 10.32604/cmc.2024.055007.
41. A. Awad, A. Ali, and T. Gaber, “An improved long short term memory network for intrusion detection,” PLoS One, vol. 18, 2023, doi: 10.1371/journal.pone.0284795.
42. A. Fataniet al., “Enhancing Intrusion Detection Systems for IoT and Cloud Environments Using a Growth Optimizer Algorithm and Conventional Neural Networks,” Sensors (Basel), vol. 23, 2023, doi: 10.3390/s23094430.
43. N. Hussen, S. M. Elghamrawy, M. Salem, and A. El-Desouky, “A Fully Streaming Big Data Framework for Cyber Security Based on Optimized Deep Learning Algorithm,” IEEE Access, vol. 11, pp. 65675–65688, 2023, doi: 10.1109/access.2023.3281893.
44. F. S. Alsubaei, “Smart deep learning model for enhanced IoT intrusion detection,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-06363-5.
45. A. Dahou et al., “Intrusion Detection System for IoT Based on Deep Learning and Modified Reptile Search Algorithm,” Comput Intell Neurosci, vol. 2022, 2022, doi: 10.1155/2022/6473507.
46. N. Dash, S. Chakravarty, A. Rath, N. Giri, K. M. AboRas, and N. Gowtham, “An optimized LSTM-based deep learning model for anomaly network intrusion detection,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-85248-z.

47. M. Y. Ayub, U. Haider, A. Haider, M. T. A. Tashfeen, H. Shoukat, and A. Basit, “An Intelligent Machine Learning based Intrusion Detection System (IDS) for Smart cities networks,” EAI Endorsed Transactions on Smart Cities, 2023, doi: 10.4108/eetsc.v7i1.2825.
48. M. N. Chohan, U. Haider, M. Y. Ayub, H. Shoukat, T. K. Bhatia, and M. F. U. Hassan, “Detection of Cyber Attacks using Machine Learning based In-trusion Detection System for IoT Based Smart Cities,” EAI Endorsed Trans-actions on Smart Cities, 2023, doi: 10.4108/eetsc.3222.
49. D. Javeed, M. S. Saeed, I. Ahmad, P. Kumar, A. Jolfaei, and M. Tahir, “An Intelligent Intrusion Detection System for Smart Consumer Electronics Network,” IEEE Transactions on Consumer Electronics, vol. 69, pp. 906–913, 2023, doi: 10.1109/tce.2023.3277856.
50. L. Idouglid, S. Tkatek, K. Elfayq, and A. Guezzaz, “Next-gen security in IIoT: integrating intrusion detection systems with machine learning for in-dustry 4.0 resilience,” International Journal of Electrical and Computer En-gineering (IJECE), 2024, doi: 10.11591/ijece.v14i3.pp3512-3521.
51. W. Rajeh et al., “Improved smart city security using a deep maxout network-based intrusion detection system with walrus optimization,” PeerJ Comput Sci, vol. 11, 2025, doi: 10.7717/peerj-cs.2743.
52. M. Darwish, M. Elsisi, M. M. Fouda, D. Mansour, and M. Lehtonen, “Emerging applications of IoT and cybersecurity for electrical power sys-tems,” IET Generation, Transmission & Distribution, 2023, doi: 10.1049/gtd2.13012.
53. K. Mekkaoui, M. Mekour, and H. Teggar, “Securing Vehicle-to-Grid Networks: A Bio-Inspired Intrusion Detection System,” Scientia Iranica, 2024, doi: 10.24200/sci.2024.64239.8820.
54. S. Chatzimiltis, M. Shojafar, M. B. Mashhadi, and R. Tafazolli, “A Col-laborative Software Defined Network-Based Smart Grid Intrusion Detection System,” IEEE Open Journal of the Communications Society, vol. 5, pp. 700–711, 2024, doi: 10.1109/ojcoms.2024.3351088.
55. N. Tariq, A. Alsirhani, M. Humayun, F. Alserhani, and M. Shaheen, “A fog-edge-enabled intrusion detection system for smart grids,” J. Cloud Com-put., vol. 13, p. 43, 2024, doi: 10.1186/s13677-024-00609-9.
56. Y. Wu et al., “Graph attention and Kolmogorov–Arnold network based smart grids intrusion detection,” Sci Rep, vol. 15, 2025, doi: 10.1038/s41598-025-88054-9.
57. F. Makhmudov, D. Kilichev, U. Giyosov, and F. Akhmedov, “Online Machine Learning for Intrusion Detection in Electric Vehicle Charging Sys-tems,” Mathematics, 2025, doi: 10.3390/math13050712.
58. S. A. Sharaf et al., “Advanced mathematical modeling of mitigating se-curity threats in smart grids through deep ensemble model,” Sci Rep, vol. 14, 2024, doi: 10.1038/s41598-024-74733-6.