

Review on Hybrid AI-Based Intrusion Detection System with Quantum-Inspired Optimization

1. Mrs. Harshitha S, Assistant Professor, CSE, Malnad College Of Engineering (Hassan)
2. Monisha K(4MC23CS096), CSE, Malnad College Of Engineering (Hassan)
3. Likitha V Kumar (4MC23CS081), CSE, Malnad College Of Engineering (Hassan)
4. Moksha R (4MC23CS095), CSE, Malnad College Of Engineering (Hassan)
5. Prathyusha V Kumar(4MC23CS121), CSE, Malnad College Of Engineering (Hassan)

Abstract -The rapid growth of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) has increased cybersecurity challenges in modern networks. IIoT environments consist of diverse and resource- constrained devices that continuously generate large amounts of network traffic. Due to weak security mechanisms and large-scale deployment, these systems are vulnerable to attacks such as zero-day attacks, distributed denial-of-service (DDoS) attacks, and advanced persistent threats. Traditional Intrusion Detection Systems (IDS), including signature-based and machine learning-based approaches, have several limitations. Signature-based IDS cannot detect unknown attacks, while standalone machine learning methods struggle with high-dimensional data, class imbalance, and nonlinear attack behaviour. To overcome these issues, researchers have proposed hybrid AI-based IDS models combining deep learning, quantum computing, and swarm intelligence optimization techniques. This paper reviews recent studies using Quantum Support Vector Machines (QSVM), transformer-based models, and optimization algorithms such as Grey Wolf Optimizer (GWO) and Salp Swarm Algorithm (SSA), highlighting their advantages, limitations, and practical challenges.

Key Words: *Internet of Things (IoT), Industrial Internet of Things (IIoT), Intrusion Detection System (IDS), Cybersecurity, Deep Learning, Quantum Computing, Quantum Support Vector Machine (QSVM), Grey Wolf Optimizer (GWO), Salp Swarm Algorithm (SSA), Hybrid AI Models*

1. INTRODUCTION

The rapid growth of IoT devices in healthcare, transportation, smart manufacturing, and energy systems has created major cybersecurity challenges. Due to limited computational power, memory, and security mechanisms, IoT devices are vulnerable to cyberattacks such as Distributed Denial of Service (DDoS), botnets, phishing, malware, and insider threats. Unlike traditional IT systems, IoT networks contain large numbers of

heterogeneous devices, making monitoring and centralized security management difficult. Such attacks can lead to data theft, service disruption, and even physical damage in industrial environments. Intrusion Detection Systems (IDS) are commonly used to detect cyber threats and are mainly classified into signature-based and anomaly-based approaches. Signature-based IDS accurately identifies known attacks but cannot detect new threats, while anomaly-based IDS can identify unusual traffic patterns but often produces high false-positive rates. To overcome these limitations, researchers have applied machine learning and deep learning techniques for traffic analysis and attack detection. However, challenges such as high- dimensional data, imbalanced datasets, noisy traffic, and limited computational resources remain significant. This paper reviews recent hybrid AI approaches that combine machine learning, quantum computing, and swarm intelligence for improved IIoT intrusion detection.

2. Literature Survey

2.1 QuIDS: A Quantum Support Vector Machine-Based Intrusion Detection System for IIoT Networks (2025)

One study introduces a security method powered by quantum computing, using what is called a Quantum Support Vector Machine. Instead of traditional methods, it shifts standard network data into a more complex mathematical environment through quantum-based kernels. Because of this shift, patterns become easier to tell apart than when using regular support vector machines in classic geometry settings. Such separation boosts how well intrusions are spotted within traffic. One part of the design handles cleaning up unprocessed network flow records before anything else happens. After that comes turning selected data features into quantum states using specialized circuits instead of combining them directly. Next step involves measuring similarities through a method based on quantum mechanics rather than classical computation. The last phase assigns labels by analyzing those measurements without relying on standard decision rules.

Tests show QuIDS spots threats more correctly while making fewer mistakes compared to older methods like support vector machines or tree ensembles. This edge appears because quantum-based similarity tools can follow tangled patterns in device communication others tend to miss.

Even with those benefits, the research comes up short in some areas. Instead of actual quantum devices, tests ran on simulated environments. Because of that gap, outcomes might shift sharply in real-world settings - noise, fading signals, and how qubits link play a big role. Another point: there wasn't enough testing on whether the system holds up when handling complex, massive IoT data flows.

2.2 Quantum-Driven Enhanced Machine Learning Algorithm for Intrusion Detection in Internet of Things Environment (2026)

The paper titled "*Quantum-Driven Enhanced Machine Learning Algorithm for Intrusion Detection in Internet of Things Environment*" [2] presents a hybrid quantum-classical intrusion detection framework. Unlike QuIDS, which replaces classical classification with quantum techniques, this study integrates quantum feature transformations into conventional deep learning workflows.

A fresh setup links quantum computing parts with convolutional neural nets, aiming to sharpen how features are pulled out while spotting bad network actions more effectively. Instead of standard methods, this blend uses quantum-powered details, leading to better F1 results when stacked against regular CNN-driven threat detectors.

This study stands out because it mixes classical and quantum methods, opening a realistic way forward for stronger digital security without needing full quantum machines. Instead of relying on pure quantum setups, it adapts existing infrastructure while still advancing protection capabilities. Nonlinear data flows gain sharper modelling, allowing the system to respond more effectively when faced with varied cyber threats. Performance holds up well even when attack types shift unexpectedly.

Even so, mixing quantum parts with regular systems makes training and running models more involved. Getting the setup to work again somewhere else isn't straightforward. What's more, there's little data on how fast it performs while operating live, raising doubts about practical use. Because it just came out, testing it on many different types of data hasn't happened yet.

2.3 Intrusion Detection System Based on Machine Learning Using Least Square Support Vector Machine (2025)

The study titled "*Intrusion Detection System Based on Machine Learning Using Least Square Support Vector Machine*" [6] presents a classical machine learning-based intrusion detection approach using Least Square Support Vector Machine (LS-SVM). What sets this model apart from others discussed here isn't a blend of quantum methods or

mixed optimization strategies. Rather, effort goes into boosting how fast it runs without losing accuracy in sorting results.

Instead of sticking to old methods, LS-SVM swaps out inequality limits for exact equalities. Because of that shift, the math simplifies straight into a set of linear equations.

Solving those means it reaches answers quicker than before.

All this trims down how much computing power it needs along the way.

When systems run low on power, this method works well in spotting break-ins. Though minimal hardware slows most tools, it keeps going without strain. Where speed counts but machines lag, it holds up under pressure. Even when memory tightens, performance stays steady. Since heavy software fails often there, lightness becomes its strength. Because scanning must continue nonstop, efficiency makes all the difference. One thing stands out - the method keeps steady results on common test sets while offering a solid reference point when stacking up hybrid against quantum-boosted intrusion detection systems. Lighter computing needs? That opens doors for smaller IoT protection setups. Still, tricky nonlinear network flows can trip it up. Why. Because older kernel designs just do not capture complex shifts well, especially when attacks change shape over time.

2.4 Large-Scale IoT Attack Detection Scheme Based on LightGBM and Improved Salp Swarm Algorithm (2024)

The paper titled "*Large-Scale IoT Attack Detection Scheme Based on LightGBM and Improved Salp Swarm Algorithm*" [3]. This approach uses LightGBM - known for speed and efficiency - not paired simply, but linked through smart integration with an enhanced version of SSA. Feature picking becomes sharper when the Improved Salp Swarm Algorithm shapes the process. Optimization doesn't follow routine paths; instead, it evolves via swarm-inspired behavior guiding LightGBM's structure. Known for speed and light memory use on structured data, LightGBM sometimes struggles if too many useless or messy columns appear in big sets. When clutter builds up, results tend to slip sideways. A refined version of the sparrow search algorithm steps in here - picking useful traits, dropping noise. Exploration across possible feature combos gets a boost, while early settling on weak choices fades out. Smart navigation tightens around what truly matters.

When tested, the system spotted things more accurately. Because of fewer features, it learned faster. Efficiency went up during training runs. Performance climbed without extra complexity tagging along. Feature choice matters more than you might think when building security tools for everyday internet devices. Not every method works well under tight computing limits found outside labs.

Even with those advantages, it lacks any touch of quantumstyle design. Because of that, what you get is still just a solid traditional technique - nothing close to a futuristic mix of AI systems.

2.5 A Novel Intrusion Detection System Based on Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer (2024)

The study “*A Novel Intrusion Detection System Based on Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer*” [4] proposes a hybrid intrusion detection framework that simultaneously addresses classification and optimization challenges. The model combines a Quantum Support Vector Machine (QSVM) with an Improved Grey Wolf Optimizer (IGWO) to enhance both feature selection and hyperparameter optimization. The IGWO algorithm is inspired by the hunting behaviour and leadership hierarchy of grey wolves. In the proposed framework, IGWO performs two major tasks: selecting optimal traffic features and tuning QSVM parameters. Unlike traditional **sequential** optimization pipelines, the proposed method jointly optimizes both processes, thereby reducing the risk of suboptimal model configuration. Experimental results show that the hybrid IGWO-QSVM model achieves higher detection accuracy, improved convergence speed, and reduced feature redundancy compared to standalone QSVM approaches. The integration of optimization and classification improves the overall efficiency of the intrusion detection process.

However, the combined use of swarm intelligence and quantum machine learning significantly increases computational complexity. In addition, the study does not adequately evaluate scalability for extremely large datasets or rapidly evolving attack scenarios.

2.6 QBCMVT: An Effective Quantum-Based Coati-MobileViT Model for Intrusion Detection in IIoT (2025)

The paper titled “*QBCMVT: An Effective QuantumBased Coati-MobileViT Model for Intrusion Detection in IIoT*” [5] presents one of the most advanced architectures among the reviewed studies. The framework combines a MobileViT transformer backbone with quantum-inspired enhancement modules and a Coati Optimization

Algorithm for feature refinement.

The study specifically targets Industrial Internet of Things (IIoT) environments, where network traffic exhibits strict latency requirements and high operational sensitivity. MobileViT employs transformer-based attention mechanisms to capture long-range contextual dependencies in network traffic sequences more effectively than traditional CNN or SVM models.

The addition of quantum-inspired modules further improves feature discrimination and representation capability.

Experimental results demonstrate very high detection accuracy in IIoT-specific datasets, highlighting the effectiveness of combining transformer architectures with quantum-inspired learning mechanisms.

Despite its strong performance, the framework introduces substantial practical challenges. Mobile ViT models require significant computational power and memory resources, making deployment on resource-constrained IIoT edge devices difficult. Furthermore, the study does not investigate model compression or quantization strategies that could improve deployment feasibility.

Table -1: Comparative Summary of Reviewed Studies

Title	Year	Model	Optimizati on	Strength	Limitation
QuIDS: QSVM-Based IDS for IIoT Networks	2025	QSVM	Quantum Kernel	High precision	Scalability issue
Quantum-Driven Enhanced ML for IIoT IDS	2026	Hybrid QNN	Adaptive	Strong nonlinear learning	High complexity
IDS Using Least Square SVM	2025	LS-SVM	Classical	Stable performance	No hybrid integration
LightGBM + Improved Salp Swarm Algorithm	2024	LightGBM	Salp Swarm	Efficient feature selection	No quantum support
Hybrid QSVM + Improved Grey Wolf Optimizer	2024	Hybrid QSVM	Improved GWO	Fast convergence	Computational overhead
QBCMVT: Quantum Coati-MobileViT for IIoT	2025	Deep + Quantum	Hybrid	High IIoT accuracy	Resource intensive

3. Dataset:

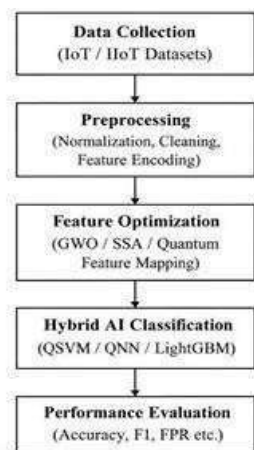
The datasets used across the six reviewed studies are summarised in Table 2. Four of the six studies use the NSL-KDD dataset or an IIoT-specific extension of it, while the remaining two rely on proprietary or domain-specific IIoT traffic captures. NSL-KDD, despite being widely used, was compiled over two decades ago and its traffic profiles do not adequately represent the diversity of modern IIoT attack vectors. Its continued dominance in IDS evaluation is a recognised limitation in the field: models that perform well on NSL-KDD have sometimes shown substantially weaker generalisation when tested on more recent datasets such as CICIDS-2018 or Bot-IIoT. Each dataset contains labelled records categorised as normal or malicious, spanning attack types including DoS, DDoS, botnet intrusion, probe attempts, remote-to-local 12 (R2L), and user-to-root (U2R) exploits. Most studies apply standard training-testing splits and some form of crossvalidation, though the depth of evaluation methodology varies. Notably, none of the reviewed papers conduct crossdataset validation, meaning it is not possible to determine whether the reported performance figures reflect genuine

generalisation capability or dataset-specific overfitting. This is one of the more important open gaps identified in this review.

Table -2: Dataset Characteristics of Reviewed Studies

Paper Title	Dataset Used	Characteristics	Evaluation Metrics
QuIDS	NSL-KDD, IoT Dataset	Multi-class attacks	Accuracy, Precision, Recall
Quantum-Driven Enhanced ML	IoT Traffic Dataset	Imbalanced traffic	Accuracy, F1-score
LS-SVM IDS	NSL-KDD	Preprocessed features	Accuracy, False Alarm Rate
LightGBM + SSA	Large IoT Dataset	High dimensional	Accuracy, Training Time
Hybrid QSVM + IGWO	NSL-KDD	Optimised feature subset	Accuracy, Convergence
QBCMT	IIoT Dataset	Industrial traffic	Precision, Recall

4. Methodology:



(Figure 1: General Methodology Pipeline for Hybrid AI-Based Intrusion Detection)

Despite the architectural diversity of the six reviewed systems, a common methodological pipeline can be identified across all studies. As illustrated in Figure 1, the pipeline consists of five major stages: data collection, preprocessing, feature optimization, hybrid AI classification, and performance evaluation. The following subsections describe each stage and highlight how the reviewed studies differ in implementation.

4.1 Data Collection

The reviewed studies utilize benchmark datasets such as NSL-KDD, IoT intrusion traffic datasets, and IIoT-specific industrial network traffic records. The datasets include multiple attack categories, including Denial of Service (DoS), Probe, Remote-to-Local (R2L), User-to-Root (U2R), botnet attacks, and Distributed Denial of Service (DDoS) attacks.

Most studies adopt training-testing splits of 70/30 or 80/20, while some employ k-fold cross-validation to improve evaluation reliability and reduce variance. Dataset selection significantly influences the reported performance of intrusion detection systems. However,

the extensive reliance on NSL- KDD remains a methodological limitation because the dataset is relatively outdated and does not fully represent modern IoT attack scenarios.

4.2 Preprocessing

Preprocessing techniques are largely consistent across the reviewed studies and typically include:

- Removal of missing or corrupted traffic records
- Elimination of duplicate entries to avoid training bias
- Conversion of categorical features into numerical representations
- Feature normalization using Min-Max scaling or z- score standardization
- Handling class imbalance through Synthetic Minority Over-sampling Technique (SMOTE) or weighted loss functions

Effective preprocessing plays a critical role in improving model convergence, classification stability, and overall detection performance. Despite its importance, several studies provide only limited details regarding preprocessing procedures, thereby reducing experimental reproducibility.

4.3 Feature Optimization

Feature optimization represents the stage where the reviewed studies differ most significantly from traditional IDS pipelines. Three primary optimization strategies are identified:

- Improved Grey Wolf Optimizer (IGWO) for simultaneous feature selection and hyperparameter tuning in QSVM-based systems
- Improved Salp Swarm Algorithm (SSA) for dimensionality reduction in LightGBM-based frameworks
- Quantum feature mapping in QSVM and hybrid quantum neural network approaches for higher- dimensional feature representation

Swarm intelligence algorithms perform heuristic exploration of the feature space to identify informative feature subsets while reducing redundancy. Although computationally efficient, these methods do not guarantee globally optimal solutions. In contrast, quantum feature mapping offers stronger theoretical representational capability for nonlinear traffic patterns but depends on quantum hardware or simulators, limiting practical deployment.

4.4 Hybrid AI Classification

After feature optimization, classification is performed using one of four major approaches: QSVM, hybrid quantum neural networks (QNNs), LightGBM, or MobileViT-based architectures. QSVM and hybrid QNN models demonstrate strong nonlinear classification capability and improved intrusion detection performance. However, these methods require higher computational resources compared to conventional machine learning algorithms. LightGBM provides comparatively efficient performance with lower computational overhead, making it suitable for large-scale IoT environments.

MobileViT-based architectures employ transformer attention mechanisms to capture long-range contextual dependencies in network traffic sequences. Although these models achieve high detection accuracy, their memory and hardware requirements limit deployment on resource-constrained IoT and IIoT edge devices.

4.5 Performance Evaluation

All reviewed studies evaluate system performance using standard intrusion detection metrics, including:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)
- Convergence speed and optimization efficiency

These metrics provide a useful basis for comparing intrusion detection models. However, most studies evaluate their systems using only a single dataset, which limits confidence in their generalization capability across diverse real-world environments.

5. Discussion and Comparative Analysis

The analysis of the six reviewed studies indicates that hybrid AI approaches integrating quantum computing, swarm intelligence, and deep learning generally outperform conventional machine learning methods in intrusion detection tasks.

What happens when quantum kernels enter the scene? Classification gets sharper. False alarms drop more than what standard SVM methods usually deliver.

The QuIDS setup shows it clearly - different paths lead to better results. Not just small gains, but noticeable shifts in performance. Instead of relying on classic patterns, a new route opens through quantum mapping. Accuracy climbs without pushing limits too hard. One change leads to another: fewer mistakes, clearer outcomes.

It looks like using more dimensions in quantum data helps tell apart signs of network intrusions better. Still, most of what we see comes from simulated setups instead of actual quantum machines.

Oddly enough, combining quantum and classical neural networks leads to better F1-scores compared to standard CNN setups. Boosts in results might come from how features are encoded into quantum states. Even so, it is still unclear whether those gains stem more from the encoding method or the overall model layout.

Out of nowhere, the LS-SVM model shows simpler methods - when tuned right - can detect intrusions just fine while using far less computing power. Suddenly, it becomes harder to ignore how much extra cost some advanced AI setups actually bring for only slight gains.

Out of all methods tested, Light GBM-SSA stands out when it comes to using group-based smarts for picking key traits. Removing unnecessary details helps speed things up while also boosting how well labels are assigned. Though simpler, the approach manages precision without extra load.

Speed gets better when features pick themselves while settings tune at the same time - this shows up clearly in IGWO-QSVM results. Still, linking quantum learning with search methods? That pushes computation costs much higher.

What stands out is how the QBCMVT system tops every other tested setup when it comes to spotting threats in industrial internet setups. Instead of just processing data separately, MobileViT uses a design based on transformers to see patterns across network activity over time. On top of that, pieces inspired by quantum computing help sharpen how features are understood. Even with those gains, actually putting it into operation remains questionable. Still causes worry because it needs so much memory and strong hardware.

7. Conclusion

One after another, the half-dozen studies pointed out weaknesses in classic intrusion detection when dealing with modern IoT needs. Faced with these shortfalls, researchers began exploring blends of artificial intelligence approaches. With quantum-inspired techniques entering the mix, collective intelligence models added extra strength. Detection rates climbed sharply - at the same time, false alerts grew far less frequent. What stayed clear was that older methods simply could not keep pace. Now deep learning stepped in, helping spot which bits of data were worth keeping. Only when everything connected did efficiency take a whole new form.

Older setups falter, yet fresh designs handle hidden cyber risks better. Rather than copying outdated methods, certain programs blend quantum concepts with clever grouping strategies. Wolves hunting in packs inspire one method - sifting through tangled information early on. Drifting plankton guide another, adjusting focus where it counts. Patterns from nature let computers see routine actions versus real trouble with sharper eyes. Out of nowhere, small vision transformers - made lean by design - spot slight changes in how factory networks move data. Not their bulk that matters, rather the way they take in surroundings, much like someone watching quietly from the edge.

Still, after gains made so far, certain hurdles refuse to fade. What catches attention most? A lot of quantum-based safety tech operates inside simulated settings instead of live quantum hardware. That gap means glitches found outside labs - like fading signals, noise from surroundings, or limits built into real gear - tend to slip through cracks. When those factors stay ignored, rolling out working versions feels uncertain, at minimum.

Apart from that, quite a few of the reviewed studies stick to one dataset - NSL-KDD shows up most often - with only a handful using even two sources

When models appear to pick up just certain patterns rather than catch breaches consistently, doubts start forming. Since performance can shift between setups, checking them on various data sets through uniform approaches helps reveal what they actually handle.

Most heavy-duty number crunching trips up hybrid quantum-classical systems. Quick threat detection in connected gadgets? That needs pace - yet low-energy units lag behind. Still, plenty of today's approaches ignore the sheer hassle of fitting them into actual environments. Consider QBCMVT: solid performance shows, but only if you accept its hunger for processing muscle - which blocks

smooth operation on edge machines until models shrink down.

Future research should focus on the following areas:

- Development of lightweight hybrid IDS architectures for IoT edge devices
- Validation of quantum-enhanced IDS models on real quantum hardware
- Standardized cross-dataset benchmarking methodologies
- Energy consumption and latency analysis for real-time deployment
- Adaptive online intrusion detection systems capable of handling evolving attack patterns

Overall, the reviewed studies establish a strong foundation for future research in hybrid AI-based intrusion detection systems. Although practical deployment challenges remain significant, the combination of quantum computing, swarm intelligence, and advanced deep learning architectures represents a promising direction for nextgeneration IoT and IoT cybersecurity solutions.

8. References

- [1] R. Kumar and M. Swarnkar, "QuIDS: A Quantum Support Vector Machine-Based Intrusion Detection System for IoT Networks," *Journal of Network and Computer Applications*, vol. 234, Art. no. 104072, Feb. 2025, doi:10.1016/j.jnca.2024.104072.
- [2] I. B. Bharathi, V. Sonai, and S. Sridevi, "QuantumDriven Enhanced Machine Learning Algorithm for Intrusion Detection in Internet of Things Environment," *EPJ Quantum Technology*, vol. 13, no. 1, Art. no. 20, Jan. 2026, doi:10.1140/epjqt/s40507-026-00463-5.
- [3] W. Chen et al., "Large-scale IoT Attack Detection Scheme Based on LightGBM and Improved Salp Swarm Algorithm," *Scientific Reports*, vol. 14, 2024.
- [4] E. I. Elsedimy et al., "A Novel Intrusion Detection System Based on Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer," *Cluster Computing*, vol. 27, 2024.
- [5] "QBCMVT: An Effective Quantum-Based CoatiMobileViT Model for Intrusion Detection in IIoT," *Computers and Electrical Engineering*, vol. 126, 2025.