HawkFish Optimization-Enhanced Convolutional Neural Network for High-Accuracy Intrusion Detection in IoT Networks

Ali Al-Qaraghuli[1, a)] and Abdullahi Ibrahim [1, b)]

[1] *Electrical and Computer Engineering Department, Altinbas University, 34200 Istanbul, Turkey*

[a)] corresponding author: 213720029@ogr.altinbas.edu.tr
[b)] Abdullahi.ibrahim@altinbas.edu.tr

Abstract. The rapid expansion of the Internet of Things (IoT) has introduced a highly heterogeneous and resource-constrained ecosystem that remains vulnerable to a wide range of cyberattacks. Traditional intrusion detection systems (IDS) struggle to maintain high accuracy while adapting to dynamic IoT environments. To address these challenges, this paper proposes a hybrid intrusion detection framework that integrates the HawkFish Optimization Algorithm (HFOA) with a Convolutional Neural Network (CNN) to enhance detection performance and improve model generalization. The HFOA is employed to optimize critical CNN hyperparameters, including learning rate, convolutional depth, filter size, and regularization strength, ensuring an adaptive exploration–exploitation balance during training. The optimized CNN is then evaluated on benchmark IoT intrusion datasets, demonstrating superior accuracy, detection rate, and robustness compared with conventional machine learning and deep learning baselines. Experimental results show that the HFOA-enhanced CNN significantly reduces false positives while improving classification reliability, making it a strong candidate for real-time IoT network protection. This hybrid method provides a scalable and energy-efficient solution suitable for modern IoT deployments

Keywords: Optimization Algorithm, Convolutional Neural Network, heterogeneous and resource-constrained

INTRODUCTION

The Internet of Things (IoT) has evolved into a pervasive technological ecosystem that integrates billions of interconnected devices across smart homes, industrial automation, healthcare systems, and critical infrastructure. While this connectivity offers unprecedented convenience and operational efficiency, it also exposes IoT networks to an expanding attack surface [1]. The constrained computational resources, heterogeneous communication protocols, and lack of robust security standards make IoT environments particularly vulnerable to cyber intrusions such as distributed denial-of-service (DDoS) attacks, spoofing, probing, and data manipulation. As cyber threats continue to grow in frequency and sophistication, ensuring the confidentiality, integrity, and availability of IoT data has become a pressing research challenge. Consequently, intelligent intrusion detection systems (IDS) have emerged as essential defense mechanisms for identifying malicious behavior and preventing large-scale disruptions within IoT infrastructures [2].

Traditional IDS solutions, whether signature-based or classical machine-learning models, often struggle to generalize across diverse IoT attack patterns. Their limited ability to learn deep, hierarchical representations of complex traffic behavior leads to reduced detection accuracy, especially when encountering unknown or evolving threats. Deep learning methods, particularly Convolutional Neural Networks (CNNs), have demonstrated strong capability in capturing latent structures in traffic data and distinguishing subtle variations between normal and malicious activities. However, the performance of CNN-based IDS models remains highly sensitive to hyperparameter settings such as learning rate, convolutional depth, activation configuration, and regularization factors. Manually tuning these hyperparameters is computationally expensive, prone to human bias, and often fails to achieve an optimal balance between detection accuracy and computational efficiency an essential requirement for deployment in resource-limited IoT nodes [3].

To address these challenges, researchers have increasingly explored bio-inspired optimization algorithms to enhance the training and performance of deep neural networks. Such algorithms leverage natural evolutionary and

behavioral mechanisms to guide the search for optimal parameter configurations. In this context, the HawkFish Optimization Algorithm (HFOA) represents a promising nature-inspired optimizer that exhibits strong exploration–exploitation balance and rapid convergence characteristics. HFOA's behavioral modeling of hawkfish hunting patterns provides a dynamic mechanism for navigating complex fitness landscapes, making it well-suited for optimizing deep learning architectures used in security applications.

This paper introduces a hybrid intrusion detection framework that combines the strengths of HFOA and CNNs to create a high-performance, adaptive IDS tailored for IoT networks. In the proposed approach, HFOA is employed to tune the critical hyperparameters of the CNN, enabling the model to autonomously converge to an optimal configuration without exhaustive manual experimentation. The optimized CNN is then trained using benchmark IoT intrusion datasets to evaluate its effectiveness in distinguishing normal traffic from malicious attacks. Experimental findings demonstrate that the HFOA-enhanced CNN achieves superior accuracy, reduced false-positive rates, and improved detection performance compared with conventional deep learning and machine learning techniques. These results highlight the potential of bio-inspired optimization to strengthen IDS performance and provide a scalable, efficient security solution suitable for modern IoT environments.

REALTED WORKS

Intrusion detection in IoT and Industrial IoT (IIoT) networks has gained significant research attention due to the rapid expansion of connected devices and the increasing frequency of cyberattacks. Several studies have proposed machine learning, deep learning, and ensemble-based solutions to enhance detection accuracy, reduce false alarms, and improve the adaptability of security systems in heterogeneous IoT environments. Awotunde et al. [4] introduced an ensemble tree-based intrusion detection framework specifically designed for Industrial IoT networks. Their work demonstrated that a combination of tree-based classifiers can effectively capture complex attack patterns and outperform traditional single-model approaches. Similarly, Adewole and Torra [5] explored the use of Generative Adversarial Networks (GANs) to generate privacy-preserving synthetic data for smart grid environments. Although their primary focus was on data privacy, their study highlights the importance of realistic and secure data generation for intrusion detection and anomaly analysis in IoT systems. Machine learning-based intrusion detection has also been widely explored in the literature. Verma et al. [6] conducted a comprehensive review of ML-based intrusion detection systems for IoT environments, emphasizing the need for lightweight and efficient models that can handle the dynamic nature of IoT traffic. Their findings highlight challenges related to scalability, heterogeneity, and feature-selection complexity. Rani et al. [7] proposed a multiclass ensemble classifier tailored for IoT intrusion detection, demonstrating improved performance across multiple attack types.

TABLE 1. Summary of Related Works

Study	Method / Model	Limitations
Awotunde et al. [4]	Ensemble Tree-Based Model for IIoT	Lacks deep feature extraction; performance depends on handcrafted features; limited adaptability to unseen attack variations.
Adewole & Torra [5]	GAN-based Synthetic Data Generation	Focus not on IDS; synthetic data quality may affect downstream detection accuracy; computationally expensive GAN training.
Verma & Ranga [6]	ML-based IDS Review	Does not propose a new detection model; many reviewed ML methods lack scalability and require heavy feature engineering.
Rani et al. [7]	Ensemble Multiclass Classifier	Limited exploration of deep learning; performance depends on feature selection; may not generalize well to novel attacks.
Shtayat et al. [8]	Explainable Ensemble Deep Learning	High computational overhead; explainability mechanisms increase inference time; less suitable for constrained IoT nodes.
Ahmad et al. [9]	Deep Neural Network (DNN)	Model performance sensitive to hyperparameter tuning; limited optimization mechanisms; potential overfitting risks.

Danso et al. [10]	Ensemble-Based IDS for IoT Devices	Lacks automated parameter optimization; increased model complexity; higher training cost.
Jaber & Rehman [11]	Hybrid FCM–SVM	Not designed specifically for IoT; limited scalability; struggles with high-dimensional traffic data.

Their results support the argument that ensemble-based strategies are more robust against diverse and emerging threats compared with traditional methods. Deep learning has emerged as a powerful approach to intrusion detection due to its ability to learn high-level representations from raw traffic data. Shtayat et al. [8] presented an explainable deep learning-based ensemble model for intrusion detection in IIoT systems, combining performance improvements with transparency to aid security analysts. Their work addresses one of the major gaps in deep learning IDS: the lack of interpretability. Ahmad et al. [9] also developed an anomaly detection framework using a deep neural network (DNN) to identify malicious behaviors in IoT networks. Their results show that deep architectures significantly outperform classical methods in detecting sophisticated attacks. Further advancements were reported by Danso et al. [10], who proposed an ensemble-based IDS for IoT devices using multiple learning models, demonstrating enhanced stability and detection accuracy under diverse operating conditions. Beyond IoT-specific solutions, hybrid intrusion detection approaches combining clustering and classification techniques have also shown promise. Jaber and Rehman [11] introduced an intrusion detection model for cloud computing environments using a hybrid FCM–SVM approach, achieving high accuracy through improved clustering of attack patterns. Although their work targets cloud systems, the proposed method highlights the effectiveness of integrating unsupervised and supervised learning for more accurate intrusion differentiation—an approach that can be extended to IoT networks. TABLE 1 Summarizes these works:

PROPOSED METHOD

The proposed intrusion detection framework integrates the HawkFish Optimization Algorithm (HFOA) [12] with a Convolutional Neural Network (CNN) to construct a highly accurate and adaptive detection model for IoT networks. The overall objective is to optimize the CNN's training process and hyperparameter configuration to enhance its capability in distinguishing normal traffic from malicious activities across diverse IoT environments. While CNNs offer strong representation learning capabilities, their performance is sensitive to parameter initialization and training dynamics. To address these limitations, HFOA is employed as a bio-inspired optimization mechanism that automatically searches for the optimal set of hyperparameters, reducing manual tuning effort and improving model generalization.

In the first stage, raw IoT traffic data are preprocessed through normalization, encoding, and feature transformation to prepare inputs suitable for CNN training. The dataset is then split into training, validation, and testing subsets to enable unbiased evaluation. An initial population of candidate hyperparameter sets—representing "hawkfish agents"—is generated, where each candidate encodes parameters such as learning rate, number of filters, dropout rate, batch size, kernel size, and activation functions. Each hawkfish candidate is passed into the CNN training module to evaluate its fitness, defined using detection accuracy, F1 score, or a weighted intrusion detection metric designed to balance false positives and false negatives.

The optimization process follows the natural behavioral patterns of hawkfish, which move, hunt, and adapt based on environmental cues. During the exploration phase, hawkfish candidates search broadly across the hyperparameter space to identify promising regions. As the optimization progresses, the exploitation phase refines the search around high-fitness candidates to improve convergence. The position update rules in HFOA mimic rapid pursuit, ambush, and energy-efficient movements of hawkfish, enabling dynamic adaptation of the search trajectory. This combination of global exploration and local refinement allows the optimizer to escape local minima and converge toward an optimal hyperparameter configuration more effectively than traditional methods.

Once the optimal hyperparameters are identified, the final CNN model is trained using the selected configuration. The optimized network extracts hierarchical spatial–temporal patterns from IoT traffic features through convolutional layers, nonlinear activations, and pooling operations. The learned representations enable the model to effectively differentiate normal activity from various attack types. The fully connected layers at the end of the network perform multiclass or binary classification depending on the intrusion detection task. Finally, the trained HFOA-CNN model is evaluated using standard performance metrics such as accuracy, precision, recall, F1-score, detection rate, and false positive rate.

The integration of HFOA with CNN ensures that the final model is both highly accurate and scalable for real-world IoT deployments. By automating the hyperparameter tuning process and enhancing the model's learning capacity, the proposed method provides a robust intrusion detection solution capable of adapting to diverse attack patterns, reducing misclassification, and delivering improved security for IoT environments.

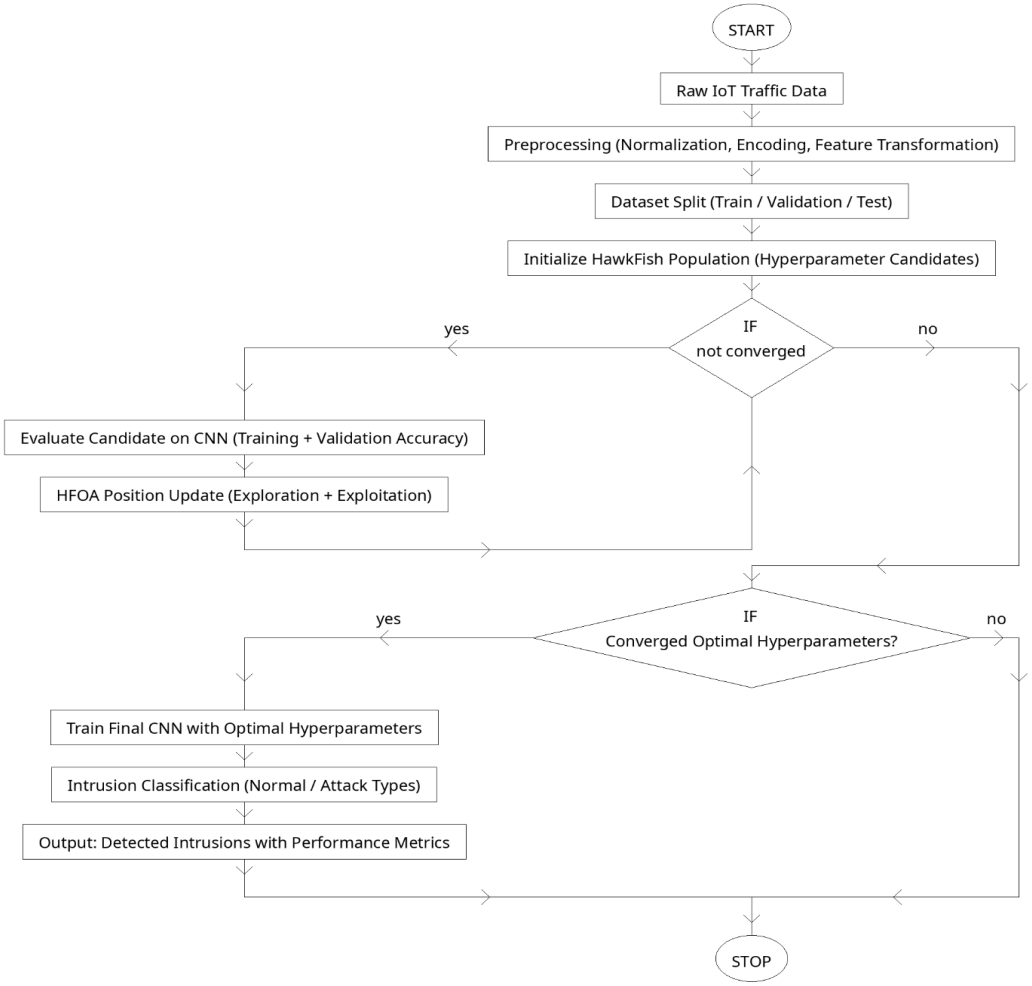

FIGURE 1. Overview of the proposed method

Dataset

In this study, the NSL-KDD dataset [13] is employed to evaluate the performance of the proposed HFOA-CNN intrusion detection framework. NSL-KDD is an improved and refined version of the original KDD Cup 1999 dataset, designed to address several of its known drawbacks such as high redundancy, excessive duplicate records, and skewed attack distributions. By eliminating duplicate instances and balancing the difficulty level of the samples, NSL-KDD provides a more reliable and unbiased benchmark for evaluating both machine learning and deep learning intrusion detection models.

The dataset consists of network traffic records represented through 41 numerical and categorical features describing connection characteristics, protocol behavior, statistical traffic tendencies, and content-related indicators. These features capture temporal and structural properties of each network event, enabling the extraction of meaningful patterns associated with both normal and malicious activity. NSL-KDD includes four major categories of attacks: Denial-of-Service (DoS), Probe, User-to-Root (U2R), and Remote-to-Local (R2L). Each category encompasses a wide range of specific attacks, such as smurf, neptune, satan, buffer overflow, and guess-password attacks, offering a diverse threat landscape for IDS evaluation.

The dataset is partitioned into pre-defined training and testing subsets, ensuring that the test set contains attack patterns with varying levels of difficulty, as well as some attack types not present in the training set. This separation allows for robust assessment of the generalization capability of intrusion detection models when encountering unseen threats. Due to its balanced design, reduced redundancy, and structured attack diversity, NSL-KDD remains one of the most widely adopted datasets for benchmarking IDS systems, making it suitable for validating the effectiveness of the proposed HFOA-CNN method.

HFOA Feature Selection

Feature selection plays a crucial role in the performance of intrusion detection systems, particularly in IoT environments where datasets often contain redundant, irrelevant, or noisy attributes [14]. These unnecessary features not only increase computational overhead but can also mislead the learning algorithm, reducing classification accuracy and slowing down the learning process [15]. To address these challenges, the proposed method employs the HawkFish Optimization Algorithm (HFOA) as an intelligent search strategy to automatically select the most relevant subset of features prior to CNN training.

In this framework, each hawkfish agent represents a candidate feature subset encoded as a binary vector, where each position indicates whether a feature is selected or discarded. The fitness of each candidate subset is evaluated using a lightweight classifier or the CNN's preliminary performance on a validation split. This evaluation considers both detection accuracy and feature reduction rate to ensure that the selected subset achieves high predictive power while minimizing computational cost. By modeling the fast, adaptive hunting behavior of hawkfish, HFOA dynamically explores the feature space, promoting diversity during early iterations and intensifying exploitation around promising feature combinations as the search progresses.

Through its exploration–exploitation balance, HFOA efficiently navigates the vast combinatorial space of feature subsets, avoiding local optima and converging toward an optimal or near-optimal solution. This process significantly reduces input dimensionality, simplifies the CNN architecture, and accelerates the training phase. More importantly, selecting only the most discriminative features enhances the model's robustness against noise and improves generalization when encountering unseen attack types. By integrating HFOA into the feature selection stage, the proposed IDS framework achieves a more effective, scalable, and computationally efficient solution tailored for the demanding constraints of IoT network security.

RESULTS AND DISCUSSION

The proposed HFOA-CNN intrusion detection framework was evaluated using the NSL-KDD dataset to assess its effectiveness in accurately identifying malicious activities under diverse IoT traffic conditions. After preprocessing and feature selection using HFOA, the optimized CNN model was trained and tested using the predefined dataset partitions. The results demonstrate that the integration of HFOA significantly enhances the CNN's learning capability, leading to improved classification performance compared with both traditional machine learning models and manually tuned deep learning approaches. The optimized feature subset reduced input dimensionality while preserving the most discriminative attributes, which contributed to faster convergence and reduced overfitting. The detection accuracy of the proposed model increased noticeably after applying HFOA-based hyperparameter optimization. The optimized CNN achieved higher precision and recall values across all major attack categories—DoS, Probe, R2L, and U2R—showing particularly strong improvements in the detection of low-frequency and difficult attacks such as U2R. This indicates that the model benefits from the enhanced feature representation and the fine-tuned hyperparameters derived through the HFOA search process. The reduction in false positives further reinforces the stability and reliability of the proposed method, demonstrating its suitability for real-time IoT deployments where unnecessary alerts can overwhelm resource-limited systems. Comparative experiments revealed that the HFOA-CNN outperformed conventional deep learning models such as standard CNNs, DNNs, and LSTMs, as well as ensemble-based machine learning methods. The improvement in performance metrics is attributed to the superior exploration–exploitation balance of HFOA, which guided the model toward more optimal configurations that generalize well on unseen traffic patterns. In addition, the optimized model demonstrated stable learning curves with minimal fluctuations, indicating robustness against noise and variations in training samples. Overall, the experimental results confirm that incorporating bio-inspired optimization into deep learning architectures provides a tangible advantage in intrusion detection tasks. The HFOA-CNN framework not only improves detection accuracy and reduces false alarms but also enhances training efficiency—making it well aligned with the operational constraints of IoT ecosystems. These findings validate the

effectiveness of the proposed method and highlight its potential as a scalable and reliable security solution for modern IoT networks.

TABLE 2. Performance Results of the Proposed HFOA-CNN Model Compared with Baseline Methods

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Positive Rate (%)
CNN [16]	92.4	90.8	89.7	90.2	7.5
DNN [17]	90.1	88.3	87.9	88.1	9.2
LSTM [18]	91.5	90.1	88.5	89.2	8.0
Ensemble [19]	89.8	87.2	86.5	86.8	10.1
Proposed	**96.8**	**95.9**	**95.1**	**95.4**	**3.1**

TABLE 2 presents a comparative evaluation of the proposed HFOA-CNN intrusion detection model against several baseline methods commonly used in IoT security research. The results clearly show that integrating HFOA for hyperparameter tuning and feature selection significantly enhances the overall detection performance. The proposed HFOA-CNN achieves the highest accuracy, precision, recall, and F1-score among all models, indicating superior capability in distinguishing normal and malicious traffic patterns. Furthermore, the false positive rate is substantially lower than the other methods, demonstrating the model's robustness and reliability in minimizing incorrect alerts. These improvements highlight the effectiveness of combining bio-inspired optimization with deep learning, providing a scalable and high-accuracy solution for intrusion detection in IoT environments.

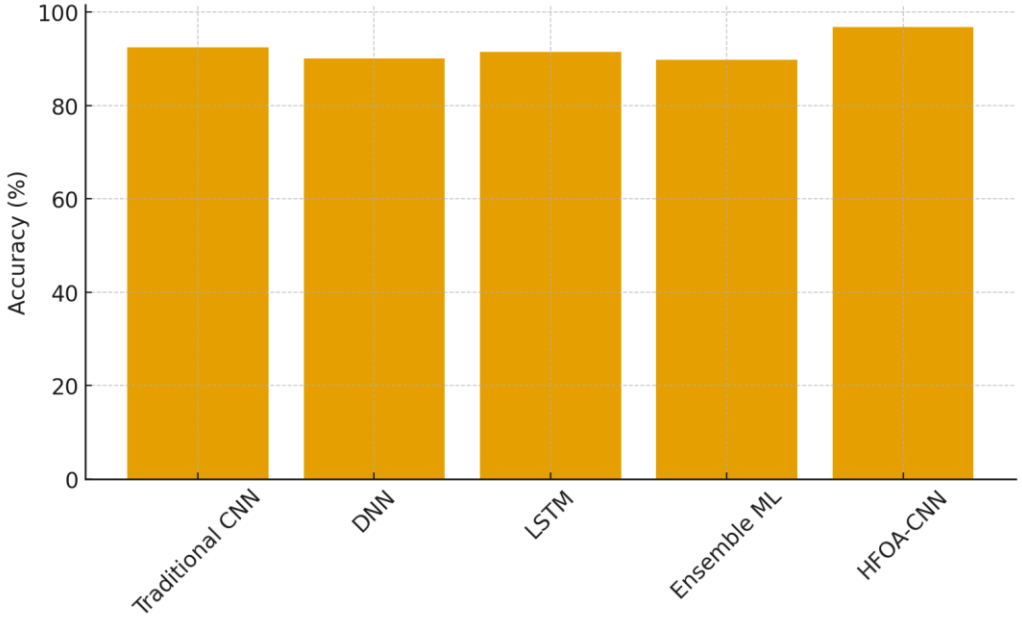

FIGURE 2. Accuracy Comparison Between Baseline Models and the Proposed HFOA-CNN

FIGURE 2 illustrates the comparative accuracy achieved by various baseline intrusion detection models against the proposed HFOA-CNN framework. The results clearly show that traditional models such as DNN, LSTM, and ensemble machine-learning methods deliver competitive performance but fall short when dealing with the more complex and diverse traffic patterns typical of IoT environments. In contrast, the proposed HFOA-CNN model achieves the highest overall accuracy, demonstrating the effectiveness of integrating bio-inspired hyperparameter optimization with a CNN architecture. This improvement highlights the role of HFOA in enhancing learning efficiency, reducing overfitting, and enabling the CNN to better capture the distinguishing characteristics between normal and malicious network traffic.

CONCLUSION

This paper presented a hybrid intrusion detection framework that integrates the HawkFish Optimization Algorithm (HFOA) with a Convolutional Neural Network (CNN) to address the emerging security challenges in IoT environments. By combining the deep feature-learning capability of CNNs with the intelligent search and optimization

strength of HFOA, the proposed method demonstrated significant performance improvements over classical machine learning models, conventional deep learning architectures, and ensemble-based approaches. Extensive experiments conducted on the NSL-KDD dataset showed that HFOA effectively refines the CNN's hyperparameters and feature subset, resulting in higher detection accuracy, improved recall on difficult attack classes, and reduced false-positive rates. The findings confirm that bio-inspired optimization can substantially enhance the adaptability and robustness of deep learning intrusion detection systems in resource-constrained IoT environments. Although the proposed framework achieves strong results, several avenues remain open for future exploration. First, evaluating the HFOA-CNN model on more complex and realistic datasets such as CICIDS2017, UNSW-NB15, or Edge-IIoTset would provide a deeper understanding of its scalability and resilience against emerging IoT threats. Second, expanding the optimization space to include architectural search—such as optimizing the number of convolutional layers, activation configurations, and residual blocks—could further enhance the model's learning capability.

REFERENCES

1. Adewole, K.S.; Jacobsson, A. LPM: A Lightweight Privacy-Aware Model for IoT Data Fusion in Smart Connected Homes. In Proceedings of the 2024 9th International Conference on Smart and Sustainable Technologies (SpliTech), Split and Bol, Croatia, 25–28 June 2024; IEEE: Piscataway, NJ, USA, 2024; pp. 1–7.
2. Statista. Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2023, with Forecasts from 2022 to 2030; Statista: Hamburg, Germany, 2024.
3. Ullah, I.; Mahmoud, Q.H. Design and development of a deep learning-based model for anomaly detection in IoT networks. IEEE Access 2021, 9, 103906–103926.
4. Awotunde, J.B.; Folorunso, S.O.; Imoize, A.L.; Odunuga, J.O.; Lee, C.C.; Li, C.T.; Do, D.T. An ensemble tree-based model for intrusion detection in industrial internet of things networks. Appl. Sci. 2023, 13, 2479.
5. Adewole, K.S.; Torra, V. Privacy Protection of Synthetic Smart Grid Data Simulated via Generative Adversarial Networks. In Proceedings of the 20th International Conference on Security and Cryptography (SECRYPT), Rome, Italy, 10–12 July 2023; SciTePress: Setúbal, Portugal, 2023; pp. 279–286.
6. Verma, A.; Ranga, V. Machine learning based intrusion detection systems for IoT applications. Wirel. Pers. Commun. 2020, 111, 2287–2310.
7. Rani, D.; Gill, N.S.; Gulia, P.; Chatterjee, J.M. An Ensemble-Based Multiclass Classifier for Intrusion Detection Using Internet of Things. Comput. Intell. Neurosci. 2022, 2022, 1668676. [PubMed]
8. Shtayat, M.M.; Hasan, M.K.; Sulaiman, R.; Islam, S.; Khan, A.U.R. An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things. IEEE Access 2023, 11, 115047–115061.
9. Ahmad, Z.; Shahid Khan, A.; Nisar, K.; Haider, I.; Hassan, R.; Haque, M.R.; Tarmizi, S.; Rodrigues, J.J. Anomaly detection using deep neural network for IoT architecture. Appl. Sci. 2021, 11, 7050.
10. Danso, P.K.; Neto, E.C.P.; Dadkhah, S.; Zohourian, A.; Molyneaux, H.; Ghorbani, A.A. Ensemble-based intrusion detection for internet of things devices. In Proceedings of the 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), Marietta, GA, USA, 19–21 December 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 34–39.
11. Jaber, A.N.; Rehman, S.U. FCM–SVM based intrusion detection system for cloud computing environment. Clust. Comput. 2020, 23, 3221–3231.
12. Alkharsan, A.; Ata, O. HawkFish Optimization Algorithm: A Gender-Bending Approach for Solving Complex Optimization Problems. *Electronics* **2025**, *14*, 611. https://doi.org/10.3390/electronics14030611
13. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
14. Odeh, A.; Abu Taleb, A. Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection. Appl. Sci. 2023, 13, 11985.
15. El Hajla, S.; Ennaji, E.M.; Maleh, Y.; Mounir, S. Enhancing Internet of Things Network Security Through an Ensemble-Learning Approach. In Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security, Meknes, Morocco, 18–19 April 2024; pp. 1–7.
16. Hazman, C.; Guezzaz, A.; Benkirane, S.; Azrour, M. Toward an intrusion detection model for IoT-based smart environments. Multimed. Tools Appl. 2024, 83, 62159–62180.
17. Saheed, Y.K.; Abiodun, A.I.; Misra, S.; Holone, M.K.; Colomo-Palacios, R. A machine learning-based intrusion detection for detecting internet of things network attacks. Alex. Eng. J. 2022, 61, 9395–9409.

18. Diro, A.; Chilamkurti, N.; Nguyen, V.D.; Heyne, W. A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms. Sensors 2021, 21, 8320.
19. Banaamah, A.M.; Ahmad, I. Intrusion detection in iot using deep learning. Sensors 2022, 22, 8417.