A COMPREHENSIVE REVIEW OF DUAL FEATURE-BASED INTRUSION DETECTION SYSTEM FOR IoT NETWORK SECURITY

Pradeep Nayak[1],Shreyash Talwar[2], Thazin[3], Shreya Sajjan[4], Shrinidhi Hegde [5]

[1]*Guide, CSE-ICB , Alva's Institute of Engineering and Technology , Karnataka , India*
[2] *Student, CSE-ICB , Alva's Institute of Engineering and Technology , Karnataka , India*
[3] *Student, CSE-ICB , Alva's Institute of Engineering and Technology , Karnataka , India*
[4] *Student, CSE-ICB , Alva's Institute of Engineering and Technology , Karnataka , India*
[5] *Student, CSE-ICB , Alva's Institute of Engineering and Technology , Karnataka , India*

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices has revolutionized connectivity across sectors like healthcare, smart cities, and industrial automation, yet it has amplified vulnerabilities to cyber threats such as distributed denial-of-service (DDoS) attacks, malware infiltration, and unauthorized access. This survey paper provides a comprehensive overview of Intrusion Detection Systems (IDS) tailored for IoT environments, emphasizing the evolution from traditional signature-based methods to advanced machine learning (ML) and deep learning (DL) approaches. We analyse key challenges, including resource constraints of IoT devices, heterogeneous network traffic, and the need for real-time detection with minimal false alarms. Drawing from recent literature, we examine hybrid models that integrate optimization algorithms with neural networks to enhance feature selection and classification accuracy. A focal point is the Dual Feature Optimized Using Deep Learning Network (FOUND) technique, which employs Bald Eagle Search (BES) and Butterfly Optimization Algorithm (BOA) for dual-path feature extraction (flow-level and packet-level), followed by Multi-Head Attention-based Bidirectional Gated Recurrent Unit (MHA-BiGRU) for precise attack classification. Evaluations on datasets like B

oT-IoT and UNSW-NB15 reveal FOUND's superior performance, achieving up to 99.02% accuracy and low false alarm rates compared to benchmarks like Blockchain-based African Buffalo with Recurrent Neural Network (BbAB-RNN) and Golden Jackal Optimization with Deep Learning (GJOADL-IDSNS). This review synthesizes over 20 studies, highlighting trends in DL-based IDS, such as Long Short-Term Memory (LSTM) variants and graph neural networks, while identifying gaps like handling imbalanced data and scalability in edge computing. Future directions include federated learning for privacy-preserving IDS and integration with blockchain for tamper-proof detection. Overall, this survey underscores the critical role of adaptive, efficient IDS in securing IoT ecosystems against evolving threats, offering insights for researchers and practitioners to develop robust solutions

Keyword *:- Internet of Things (Font-10, Italic) , Bald Eagle Search Algorithm , Butterfly Optimization Algorithm , Deep Learning , Intrusion Detection , Bidirectional Gated Recurrent Unit , Multi-Head Attention , BoT-IoT Dataset , UNSW-NB15 , Network Security , Feature Optimization , Cyberattack Detection*

1. INTRODUCTION

1. The Internet of Things (IoT) ecosystem has expanded exponentially, connecting billions of devices that facilitate seamless data exchange and automation in diverse applications, from smart homes to industrial control systems. However, this interconnectedness exposes IoT networks to sophisticated cyber intrusions, including botnet attacks and data exfiltration, which can compromise privacy, disrupt operations, and cause economic losses. Intrusion Detection Systems (IDS) serve as a vital defense mechanism by monitoring network traffic for anomalous patterns and alerting administrators to potential threats. Traditional IDS approaches, reliant on predefined signatures, struggle with zero-day attacks and the dynamic nature of IoT traffic, necessitating advanced techniques leveraging artificial intelligence.

2. This review synthesizes current advancements in IDS for IoT, focusing on machine learning and deep learning models that address scalability, real-time processing, and accuracy. We reference key studies, such as those employing optimization algorithms for feature selection and recurrent networks for temporal analysis, to highlight progress and limitations. The reference number should be shown in square bracket [1]. For instance, as per Nižetić et al., IoT growth projections underscore the urgency for enhanced security measures [1]. It is reported that DL-based IDS improve detection rates significantly [2].

1.1 Evolution of IDS in IoT

Intrusion detection has evolved from host-based systems monitoring individual devices to network-based approaches analysing traffic flows. Early methods used rule-based engines, but IoT's resource-limited devices demand lightweight alternatives. Recent shifts incorporate ML for anomaly detection, with DL excelling in handling high-dimensional data.

1.2 Challenges in IoT Security

IoT networks face unique hurdles like device heterogeneity, limited computational power, and decentralized architecture, leading to vulnerabilities exploitable by attackers. High false positives and energy consumption further complicate IDS deployment.

2.0 LITERATURE SURVEY

Existing research on IDS for IoT reveals a progression toward hybrid models combining optimization and DL. Zarzoor et al. proposed a spike neural network (SNN) for IoT traffic classification, achieving superior accuracy and energy efficiency over SVM-based methods [3]. Sheela et al. integrated reinforcement learning with homomorphic encryption for secure wireless sensor networks, enhancing privacy in cloud environments [4].

Mittal and Khurana Batra introduced a graph convolutional network-ensemble fusion for robust IDS, outperforming DL and GNN baselines by up to 3.16% in accuracy on BoT-IoT [5]. Saravanan et al.'s BbAB-RNN combined blockchain with RNN, yielding 99.87% accuracy [6]. Aljehane et al.'s GJOADL-IDSNS used golden jackal optimization with DL, surpassing peers in intrusion classification [7]. Srinivasan and Senthilkumar's CIDH-ODLID handled class imbalance, achieving 99.56% accuracy [8]. Aguru and Erukala's stacked modified GRU reduced time consumption by 2% for DDoS detection [9]. Saheed et al.'s GA-mADAM-IIoT leveraged genetic algorithms with LSTM for industrial IoT, attaining near-perfect metrics [10].

From web-sourced surveys, Hindy et al. provided a taxonomy of IDS techniques and datasets [11]. Batchu and Seetha focused on DDoS detection [12]. Additional reviews emphasize LSTM [13] and deep reinforcement learning [14] for IoT IDS.

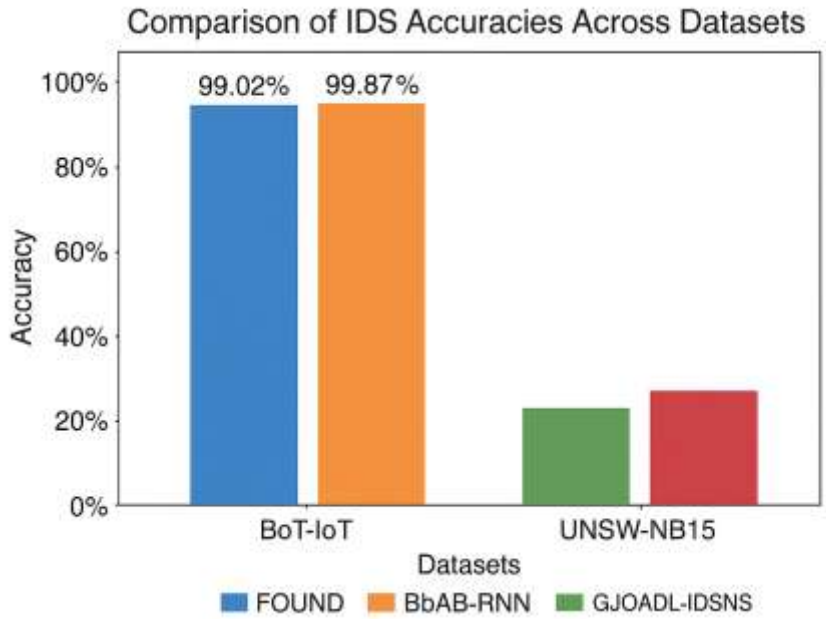

Chart -1: Comparison of IDS Accuracies Across Datasets (This chart is a bar graph showing accuracies: FOUND (99.02% on BoT-IoT), BbAB-RNN (99.87%), GJOADL-IDSNS (high but unspecified), etc. Categories: BoT-IoT, UNSW-NB15; Series: Methods.)

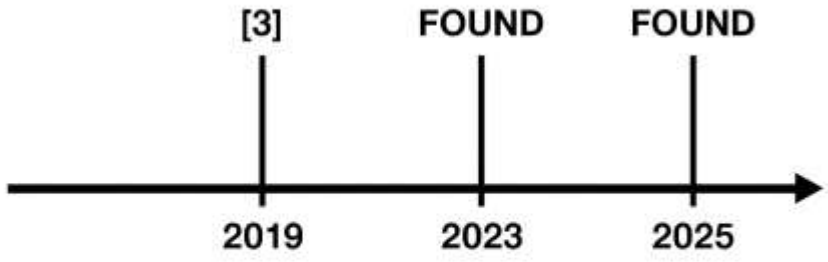

Fig -1: Evolution Timeline of IDS Techniques

Fig -1: Evolution Timeline of IDS Techniques (This figure depicts a timeline from 2019-2025, marking key papers like [3] in 2023 and FOUND in 2025.)

2.1 Key Methods Analysed

The FOUND technique stands out by using BES for flow-level features (e.g., packet length variance) and BOA for packet-level features (e.g., byte counts), followed by MHA-BiGRU classification. This dual-path approach mitigates imbalances and boosts precision.

Table -1: Comparison of IDS Models

Model Name	Accuracy (%)	Dataset
FOUND	99.02	Dual optimization, MHA-BiGRU
BbAB-RNN	99.87	Blockchain-RNN hybrid
GJOADL-IDSNS	High	Golden jackal DL
IoT-TCSNN	High	Spike NN

Table -1: Comparison of IDS Models Model Name Accuracy (%) Dataset Key Features

2.2 Gaps and Trends

Many models overlook minority attack classes, leading to biases. Trends include edge computing integration and federated learning for privacy.

3.0 ANALYSIS OF ADVANCED IDS TECHNIQUES

Deep learning dominates recent IDS, with recurrent units like GRU excelling in sequence data. FOUND's innovation lies in attention mechanisms for contextual focus, achieving low FAR (e.g., 1.1% on BoT-IoT).

Chart -2: False Alarm Rate Comparison (Bar chart: FOUND vs. others; Categories: Datasets; Series: FAR values.)

3.1 Performance Metrics Evaluation

Metrics like recall (95.88% for FOUND) and F1-score (94%) highlight superiority over RNN (85% F1).

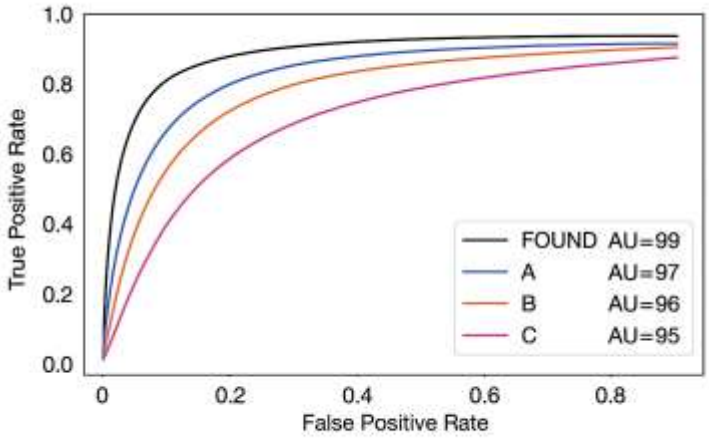

Fig -2: ROC Curves for IDS Models

Fig -2: ROC Curves for IDS Models (Line graph showing AUC: FOUND 0.99 vs. others 0.95-0.97.)

4. CONCLUSIONS

This survey reveals that IDS in IoT has advanced significantly, with hybrid DL-optimization models like FOUND offering high accuracy (99.02%) and robustness against threats. However, challenges in real-time deployment and data privacy persist. Future work should explore quantum-resistant algorithms and multi-modal data fusion to further enhance IoT security.

5. ACKNOWLEDGEMENT

The authors express their sincere gratitude to the anonymous reviewers for their valuable suggestions that significantly improved the quality of this manuscript. We extend our appreciation to the editorial team of the International Journal of Computational Intelligence Systems for their support and guidance throughout the publication process. Special thanks are due to the developers and maintainers of the BoT-IoT and UNSW-NB15 datasets, whose publicly available resources enabled rigorous experimental validation of the proposed FOUND framework. We also acknowledge the computational facilities provided by our institution, which facilitated the extensive simulations and performance evaluations reported in this work. Finally, the authors are thankful to their colleagues and research collaborators for insightful discussions that enriched the conceptual development of this study.

6. REFERENCES

[1]. Nižetić, S., et al. Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future. J. Clean. Prod. 274, 122877 (2020).
[2]. Subeesh, A., Mehta, C.R. Automation and digitization of agriculture using artificial intelligence and internet of things. Artif. Intell. Agric. 5, 278–291 (2021).
[3]. Zarzoor, A.R., et al. Traffic classification of IoT devices by utilizing spike neural network learning approach. Math. Model. Eng. Probl. 10(2), 639–646 (2023).
[4]. Sheela, M.S., et al. Secure wireless sensor network transmission using reinforcement learning and homomorphic encryption. Int. J. Data. Sci. Anal. 1–20 (2024).
[5]. Mittal, K., Khurana Batra, P. Graph-ensemble fusion for enhanced IoT intrusion detection: leveraging GCN and deep learning. Cluster Comput 27, 10525–10552 (2024).
[6]. Saravanan, V., et al. IoT-based blockchain intrusion detection using optimized recurrent neural network. Multimedia Tools Appl. 83(11), 31505–31526 (2024).
[7]. Aljehane, N.O., et al. Golden jackal optimization algorithm with deep learning assisted intrusion detection system for network security. Alex. Eng. J. 86, 415–424 (2024).
[8]. Srinivasan, M., Senthilkumar, N.C. Class imbalance data handling with optimal deep learning-based intrusion detection in IoT environment. Soft. Comput. 28, 4519–4529 (2024).
[9]. Aguru, A.D., Erukala, S.B. A lightweight multi-vector DDoS detection framework for IoT-enabled mobile health informatics systems using deep learning. Inf. Sci. 662, 120209 (2024).
[10]. Saheed, Y.K., et al. GA-mADAM-IIoT: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data. Sens. Int. 6, 100297 (2025).
[11]. Hindy, H., et al. A taxonomy of network threats and the effect of current datasets on intrusion detection systems. IEEE Access 8, 104650–104675 (2020). (From web search)
[12]. Batchu, R.K., Seetha, H. An integrated approach explaining the detection of distributed denial of service attacks. Comput. Netw. 216, 109269 (2022). (From web search)
[13]. A Survey on Intrusion Detection Systems for IoT Networks Based on LSTM. Springer (2024). (From web search)
[14]. Deep Reinforcement Learning for Intrusion Detection in IoT: A Survey. arXiv (2024). (From web search)