Communications in Mathematics and Applications
Vol. 16, No. 2, pp. 543–556, 2025
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v16i2.3008

http://www.rgnpublications.com

Research Article

An Enhanced Intrusion Detection Classification Approach for Securing IoT Networks

Fayez Alharbi

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia
fs.alharbi@mu.edu.sa

Received: January 22, 2025 **Revised:** March 17, 2025 **Accepted:** April 8, 2025

Abstract. The research investigates different classification methods that IDS developers use for developing intrusion detection systems. Recent rapid growth of internet of things (IoT) devices created a massive surge in available data requiring highly effective methods for preventing malicious activities. The research attempts to boost IDS effectiveness through ML algorithm implementation to obtain precise intrusion classification and identification. The research group obtained assessment data through three datasets which included IoT-Modbus and IoT-Fridge and IoT-Weather to measure classification frameworks' abilities when detecting different threats affecting IoT systems. For the IoT-Fridge dataset, the one-vs-one (OvO) classification reached 100% accuracy; for the IoT-Weather and IoT-Modbus, the accuracy was 99.7% and 77.62%, respectively. The one-vs-rest (OvR) classification method yielded accuracies of 100% for IoT-Fridge data, 98.02% for IoT-Weather, and 77.62% for IoT-Modbus. The performance results on IoT-Modbus and IoT-Fridge datasets were comparable between OvO and OvR methods while OvO produced slightly superior results on the IoT-Weather dataset. The research demonstrates that multi-class classification techniques demonstrate outstanding performance for IDS systems which can boost IoT application cybersecurity capabilities. The major objective of this research is to introduce a new IDS system with enhanced potential of detecting threats in IoT environments, while handling specific IoT protection obstacles.

Keywords. Intrusion detection, Internet of Things, Classification, Cybersecurity, Data breaches

Mathematics Subject Classification (2020). 68T05, 68M12, 62H30, 94A60

1. Introduction

The vast digital world allows the IoT to influence our daily lives as it automates the management of devices along with deployment of automated processes. Rapid technological development across our contemporary society generates extremely intense security issues particularly for cyber systems. IoT systems generally possess weak security systems that expose their connected devices to penetration attempts from network-based and insiders' threats. The rate at which vulnerability increases has compelled IDS to become the frontline defense. The future efficiency of IDS systems hinges on their continuous development because cyber-attacks still increase in their sophistication in nature. The emergence of ML is a proactive approach to enhancing IDS capabilities because it provides enhanced tools in detecting and controlling security threats in an efficient and accurate manner. Multi-class classification demonstrates impressive potential in ML due to its capacity to analyze complex data belonging to more than one category (Alsaedi *et al*. [4], and Tiwari *et al*. [25]). In the context of IoT intrusion detection it becomes crucial to possess this feature since attacks have significant variations in their complexity levels. Application of multi-class classification allows models to define accurate intrusion categories while handling large and heterogeneous dataset collections. The two commonly employed classification methods are OvR and OvO techniques. IoT security protocols increasingly rely on OvO methods among their implementation methods. With its OvR method the problem gets fragmented into a collection of binary classification tasks which determine if particular classes exist or not. The class assignment took place by relying on the decision from the most confident classifier. Using OvO methodology develops separate classifiers between all possible class combinations which let the sub-class determine the final outcome between pair classes through pairwise comparison scores. The combination of these two approaches provides unique functionalities that are well-tailored for addressing the operational needs of IoT-ID (Elnakib *et al*. [9]). The key goal of this work is to overcome the gaps that exist in the current *Intrusion Detection System* (IDS) deployments by performing multi-class classification on multiple TON-IoT datasets and creating a more agile and robust IDS that can effectively detect and classify a variety of cyber threats. Even though industrial sensor networks and the associated devices play a critical role in the industry, they have also caused great concerns due to sudden data transmission rate increases. Due to their networked nature, these devices, ranging from home appliances to essential industrial controls, have multiple potential entry points across diverse cyber threatspresent-day cyber threats are characterized by dynamism and complexity; thereby, traditional IDS paradigms that rely on static, rule based detection practices are not effectively dealt with when addressing these evolving threats, This necessity is recognized as a critical factor driving the shift toward the intellectualization of IDS paradigms, where smarter and more dynamic approaches are adopted to interpret the highly complex patterns that define modern cyber threats.Cross-training with machine learning could accelerate and expand the horizons of IDS systems particularly with the help of multi-class classification problems. Multiple threat-classing approaches enable the cybersec professionals to categorise the cyber threats into certain grouping systems that accelerate their response operations. AIML models better comprehend the attack descriptions and thus contribute towards the formulation of proactive threat-prevention policies. Incorporating the latest ML models into the framework of the IDS offers scalable security policies along with their high detecting abilities and thus forms an effective security protocol. Training the ML detecting mechanisms to refrain from fooling the security mechanisms requires high-dimensional datasets such as the TON-IoT dataset.

It is possible for the model to detect risk attributes through the process of feature-selection integration with dimensionality-reduction optimisation of the dataset. Besides the features previously mentioned, the approach works towards the enhancement of accuracy in the detection of IoT attacks and towards reducing the operational expenditures, thereby enabling equitable solutions to suit IoT networks with limited resources. In addition, the explainability methods such as the SHAP (*SHapley Additive exPlanations*) work towards the realised interpretability of the models. Since the incorporation of SHAP renders categorisation choices interpretable, automated IoT mechanisms can be relied on as well as transparent. Through the development of ML models and advanced multi-class classification techniques, IDS protocols are positioned as proactive and adaptable security defenders against online threats. By resolving the existing problems with IoT and Ton-IoT frameworks, it is possible to provide a strong basis for protecting IoT ecosystems, which continue to be a driving force behind the development of dependable technologies without compromising cybersecurity protocols. As machine learning techniques evolve, they aim to address the shortcomings of current security models and enable the creation of innovative, reliable, and secure IoT ecosystems. By ensuring that security is maintained, they want to contribute to the development of IoT networks, allowing companies and interested researchers to fully embrace linked technology (Qawqzeh *et al*. [15]).

2. Literature Reviews

A number of related studies, e.g., Priya *et al*. [13], Singh and Ujjwal [23] offer insightful information on the IoT environment by examining applications meant to improve their viability, affordability, and efficiency in practical applications. IoT devices are susceptible to persistent assaults, though, because they frequently function in unmonitored settings. In IoT contexts, the likelihood of a hacker obtaining direct access to IoT equipment emphasises the critical need for dependable and trustworthy IDS. Several similar efforts focused on the creation of machine learning classifiers to identify and anticipate such breaches, using a variety of methods to improve IoT security. *IoT and industrial-IoT* (IIoT) sensor datasets are publically available, and one line of study attempted to assess the performance metrics of several ensemble-ML algorithms for classification issues using these datasets (Qawqzeh *et al*. [17]). Detect, an ML-based tool for detecting vulnerabilities in IoT systems was presented by Rani *et al*. [19]. Current network classification strategies were evaluated by Al-Boghdady *et al*. [2], looking at approaches including deep packet analysis and port-based categorisation. Azab *et al*. [5] used convolutional neural networks (CNNs) to extract significant features with the goal of reducing dimensionality to create meaningful input representations. Similar findings were reported by Dahou *et al*. [8], where it was suggested that deep learning processors significant potential to enhance IoT security. A further notable study by Yaras and Dener [28] proposed a multi-layered intrusion detection approach, in which the first stage was designed to identify the presences of intrusions, while the second stage was aimed at determining the specific type. This procedure was performed through oversampling to improve both accuracy and reliability. It was identified that only system be developed to maintain high levels of security that minimize the probability of suspicious activities, but it is also essential that research be conducted on IoT technologies to enable the detection and prediction of potential frauds. Classification models were additionally developed to process the input of IDS (Khan *et al*. [11], Srikanth [24], and Shirodkar [22]). The paper is composed of several datasets containing attack frames from various IoT systems that operate using the MQTT protocol within the scope of this research.

Therefore the present study is focused on the continuous efforts to enhance IoT security metrics through advanced ML algorithms and IDS development initiatives. The rapid advancement of IoT network implementations has, in turn, provided distinctive capabilities for intelligent applications aimed at improving operational efficiency across multiple industries. However, this expansion has also introduced numerous complex challenges concerning security, particularly in the context of intrusion detection scenarios, Indeed, recent literature has been largely dedicated to the utilization of machine learning and deep learning techniques to address security related challenges through the design of optimized intrusion detection detection system application in IoT environments (Alaiz-Moreton *et al*. [1]). One particularly innovative development has been the DL-based detection system, which has been optimized and deployed at the edge of IoT networks. In this approach, DL algorithms are applied to categorize security and to identify anomalies through real-time analysis of IoT data (Rani *et al*. [19]). The deployment of such systems at the edge ensures the real-time functionality of IDS and provides improved responsiveness over time a factor that can prove decisive in time sensitive circumstances.

More analysis of the energy consumption and *Quality of Service* (QoS) in self-aware networks, could thus be performed. The self-monitoring and self-optimizing methods would therefore allow such networks to adapt automatically to the evolving situations and possible future cyberthreats as a consequence of their adoption of themselves in practice (Shirodkar [22]). ML model integration, therefore, becomes a crucial aspect of the sustainability of the Internet of Things as it predicts and reduces security risks, as well as ensures performance and energy efficiency. Various methods including neural networks, Bayesian networks, and hidden Markov models have been employed to distinguish between anomalous and normal behavior in the IoT networks in the IoT ecosystem. Other methods that have been used recently to identify anomalies in the Internet of Things are CNNs and *Simple Recurrent Units* (SRUs) (Churcher *et al*. [7]). Indeed, these models did a good job in terms of the complexity of data analysis to improve intrusion detection in the Internet of Things environment. Another concept that has raised much interest in the future security models that can be used to keep pace with the dynamic nature of the IoT ecosystems is real-time adaptive security. This type of system uses machine learning algorithms to learn network traffic behaviour to identify known and unknown security threats automatically. That is, these solutions guarantee rapid response to threats in IoT networks, which makes the transfer of IoT data smooth. Another example of innovation is the use of *Unmanned Aerial Vehicles* (UAVs) in *Intelligent Transportation Systems* (ITS). The sensors and communication features of the UAVs can be applied to numerous applications, such as data gathering, support of traffic management, and monitoring of traffic conditions. To guard against potential cyberthreats that might attack the communication channels between UAVs and ground applications, it is necessary to have more dependable *intrusion detection systems* (IDSs). In addition, the convergence of Industry 5.0 and the Internet of Things led to the production of factories and warehouses. These settings depend on IoT devices to monitor and regulate operations, which leaves them open to cyberthreats (Qawqzeh and Samaraa [16]).

By identifying and mitigating potential attacks in real-time, IDS implementation utilising ML models may therefore greatly enhance the security features of these systems. When accomplished, this guarantees the safety and continuation of industrial processes. Another use of IoT devices is the monitoring and data collection of patients in healthcare institutions. Therefore, protecting sensitive patient data requires that IoT devices be secured. Recent research has concentrated on creating customised IDS for healthcare IoT systems (Sarhan *et al*. [21], and Qawqzeh *et al*. [18]). They used machine learning algorithms to identify irregularities, protecting patient health information and guaranteeing compliance with national and international healthcare laws. In conclusion, dependable IDS development for IoT environments has advanced significantly during the past five years. By combining ML and DL approaches, these systems are now better equipped to identify and counteract a variety of cyberthreats (Le *et al*. [12]). The significance of optimising these systems for energy efficiency, real-time applications, and flexibility to changing landscapes in IoT technologies is still being emphasised by the current research orientations.

3. Research Methodology

Using OvO and OvR multi-class classification approaches for IDS creation in an IoT setting, this work employs a systematic methodology to evaluate and compare performance measurements. Figure 1 below illustrates the technique, which consists of data collection, preprocessing, classifier training, and performance evaluation.

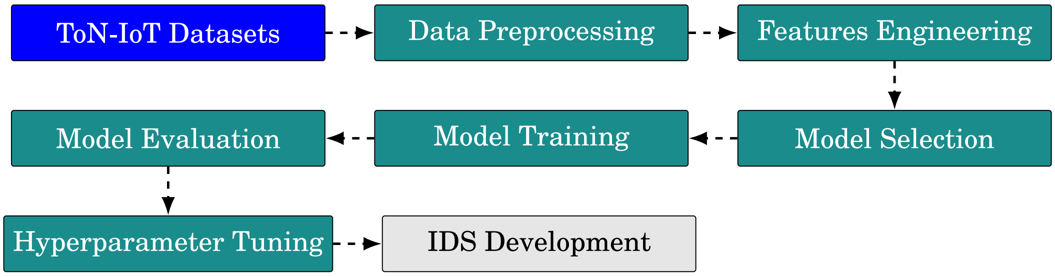


Figure 1. Multi-class classification research method

Both OvO and OvR methods were applied independently to predict the target classes of multiple IoT datasets. For OvO classification, the required number of binary classifiers was determined using:

$$\text{OvO}_{\text{\_classification}} = \left(N * \frac{N-1}{N}\right). \tag{3.1}$$

The sentence states that N is the number of subclasses that are present in the target classes. OvR classification relied on the use of N binary classifiers, which were trained to distinguish one class from every other class. For each dataset, Table 1 provides a summary.

Table 1. The description of the used ToN_IoT Datasets

Dataset Name	Data_Shape	Output Classes
IoT-Modbus	(287,194,7)	Password, Injection, XSS, Backdoor, Scanning, Normal
IoT-Fridge	(587,076,5)	Normal, Ransomware, XSS, Backdoor, Password, DDoS, Injection
IoT-Weather	(650,242,6)	Normal, DDoS Ransomware, Password, XSS, Injection, Scanning, Backdoor

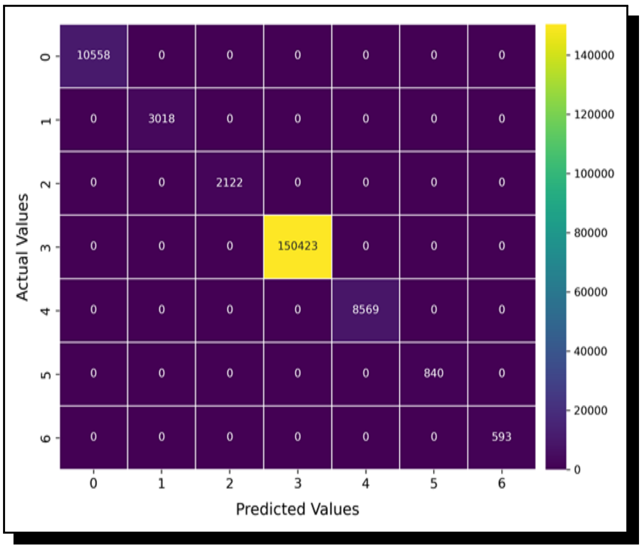
A normalizing process applied to numerical features along with target variable encoding preceded training subset and testing subset creation with their 80 : 20 ratio distribution. The performance measures of OvO and OvR classifier in training were accuracy and the measurement of recall and precision and F1-score. The researchers implemented this approach to evaluate the performance of intrusion detectors in the IoT setting through their classifiers. This paper reviews various methods by comparing them to identify the most appropriate multi-class classification method that can enhance the IDS systems in the IoT setups.

The research methodology includes some extra steps to address significant challenges in the process of multi-class classification operations in IoT settings. The methodology involves the analysis of dataset characteristics particularly data complexity along with class imbalance and overlapping features that influence the model performance outcomes. The method uses SMOTE (Synthetic Minority Oversampling Technique) and synthetic data augmentation capabilities to address the problem of class imbalance and provide adequate class distribution (Ullah *et al*. [26], and Alotaibi *et al*. [3]). These techniques are necessary to prepare datasets since they create balanced datasets that can be used to create reliable machine learning models. These preparation steps enable the methodology to provide models with enhanced capabilities to operate with diversified complex IoT data resulting in enhanced target subclassification accuracy. Complex hyperparameter optimization methods that are specific to each dataset are critical to the methodology to optimize models since they enhance model performance. The need to maintain the best configurations in the IoT-Fridge dataset and conduct validation on other datasets is still necessary. The accuracy difference between OvO and OvR shows why the choice of algorithm must take into account the complexity of the dataset to make predictions (IoT-Weather had 99.7% success with OvO and 98% with OvR). The confusion matrices that were followed to conduct a deep analysis of the misclassification patterns because they specifically impacted the IoT-Modbus dataset. The refining process of the model involved several rounds of testing of new features and combinations of them to further improve performance. This study compared the performance of OvO and OvR models in terms of execution to ensure that the chosen methodology remains feasible in the actual implementation of IoT. The research methodology finishes an iterative model refinement procedure that introduces solutions to dataset-specific issues to determine an effective IDS framework that can be used to provide stable and efficient IoT monitoring systems with different datasets.

4. Results and Discussions

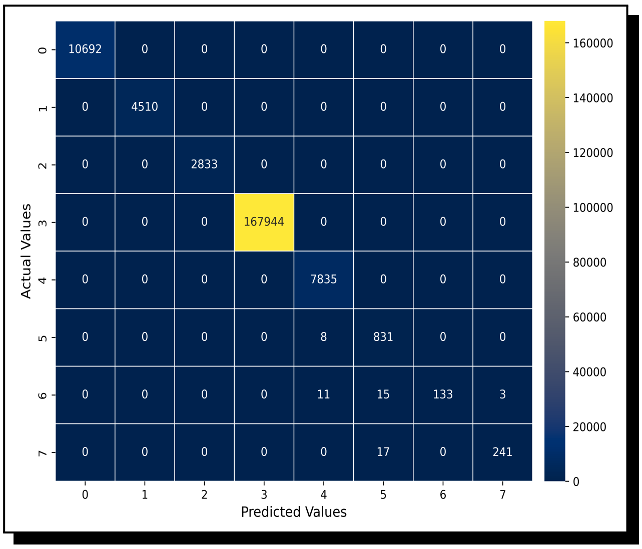
Multi-class classification has been conducted on three IoT data sets, i.e., IoT-Fridge, IoT-Weather, and IoT-ModbusAfter the classification models were trained, various subsets were tested by the researches and the results were summarized in Table 2. The state-of-the-art performance under the dataset is shown through the analysis which reveals significant insights into the merits and demerits of the models to be applied in the future. From the analysis of these outcomes, essential knowledge is derived that can be utilized by teams to enhance capabilities more suitable for real-world IoT security application. Perfect classification accuracy is achieved by the model when various data patterns are identified, leading to completely error-free intrusion type classification. The obtained performance level is demonstrated to reflect the reliability and stability of these models, as well as their potential for real-world intrusion detection system requiring high accuracy. On the IoT Weather dataset, exceptional results were achieved, with OvO found to slightly outperformer OvR. An accuracy of 99.9% was reported for OvO, while OvR followed closely with 98%. The effectiveness of these classification methods is demonstrated experimentally especially in situations where datasets contain multiple intrusion categories with complex relationships and patterns. The slight advantage observed for OvO is considered evidence that it can be applied more efficiently and innovatively in scenarios requiring precise differentiation between closely related classes.

The very high accuracy means that models can readily handle these complex IoT data at a very low error rate and then confirm their usefulness in Internet of Things applications that are security sensitive. Both the IoT-Modbus dataset under OvO and OvR achieved an accuracy of 77.62% which is rather high and even more impressive than the other datasets. The IoT-Modbus dataset analysis performance results were lower than others, which proves its problematic character, and the potential causes include the difficulty of classification, overlapping features, and the lack of difference between classes. Thus, as the performance was low, additional preprocessing methods should be used, such as certain advanced feature engineering and data augmentation with oversampling methods, such as SMOTE, to resolve the problem of class imbalance. Despite the challenges that were encountered, we believe that the model is significant and can be used to come up with improved models in the near future. The model performance evaluation also involved the confusion matrices of each dataset that helped to identify certain patterns of failure. The confusion matrices proved that the amount of misclassified instances in IoT-Fridge and IoT-Weather datasets was small, or, in other words, that the models were observed to be working well on these systems. The matrices obtained with the help of the IoT-Modbus data show that there were some areas that were problematic to the model as it attempted to differentiate subclasses that had overlapping features. The study shows the importance of future model optimization work in order to define the improved discrimination ability of closely related categories. Outstanding results in IoT intrusion detection system are yielded by the OvO and OvR classification methods when datasets with distinctly separated patterns are applied. High accuracy is achieved because the IoT-Fridge and IoT-Weather datasets are tested, indicating that practical applications of these models are demonstrated even though the IoT-Modbus results reveal missed opportunities for performance improvement. The issues of class imbalanced and feature overlap in the IoT-Modbus dataset are planned to be addressed within the model so that its performance can be enhanced. The essential role of multi-classification systems in IoT defense mechanism is emphasized by the research, and a fundamental framework for developing dependable intrusion detectors is presented. Studies of this assessment and future improvements contribute to developing security protocols which effectively fight complex and changing cybersecurity threats for IoT networks. The research compares its findings to previous studies in Table 3 thus showing what has been achieved and identifying directions for upcoming work. Through Figures 2 to 4, the OvO confusion matrix assessment results display data for the IoT-Light, IoT-Weather, and IoT-Modbus datasets. Research results on leveraging IoT datasets for multiclass classification models to justify their performance requirements are shown in Table 2. Table 3 provides comprehensive information about multi-class classification Reports through the combined use of OvO and OvR models.



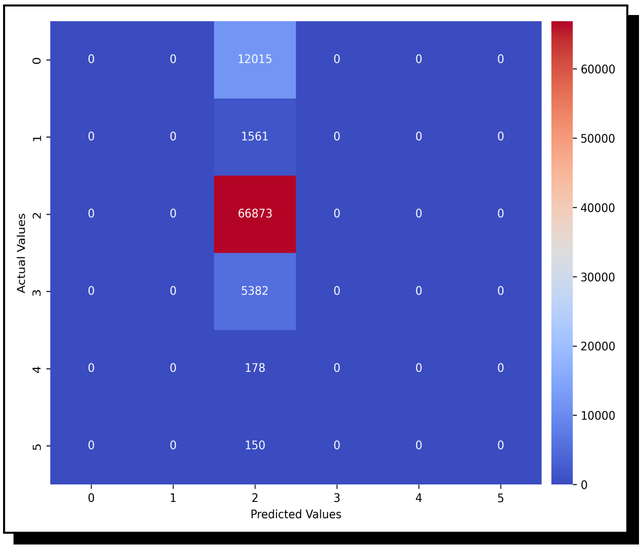
	0	1	2	3	4	5	6
0	10558	0	0	0	0	0	0
1	0	3018	0	0	0	0	0
2	0	0	2122	0	0	0	0
3	0	0	0	150423	0	0	0
4	0	0	0	0	8569	0	0
5	0	0	0	0	0	840	0
6	0	0	0	0	0	0	593

Figure 2. The IoT Fridge dataset's OvO-based confusion matrix



	0	1	2	3	4	5	6	7
0	10692	0	0	0	0	0	0	0
1	0	4510	0	0	0	0	0	0
2	0	0	2833	0	0	0	0	0
3	0	0	0	167944	0	0	0	0
4	0	0	0	0	7835	0	0	0
5	0	0	0	0	8	831	0	0
6	0	0	0	0	11	15	133	3
7	0	0	0	0	0	17	0	241

Figure 3. The OvO-based Internet of Things weather confusion matrix



	0	1	2	3	4	5
0	0	0	12015	0	0	0
1	0	0	1561	0	0	0
2	0	0	66873	0	0	0
3	0	0	5382	0	0	0
4	0	0	178	0	0	0
5	0	0	150	0	0	0

Figure 4. The confusion matrix of OvO-based IoT-Modbus

Table 2. Comparison of Studies Using IoT Datasets for Multiclass Classification Models

#	Reference	Title	Year	Results
1	Elnakib *et al.* [9]	EIDM: Deep learning model for IoT intrusion detection systems	2023	The EIDM model achieved 95% accuracy in classifying cyber-threats
2	Yaras and Dener [28]	IoT-based intrusion detection system using a new hybrid deep learning algorithm	2024	Overall accuracy 98.75% (binary classification) on the TON-IoT dataset
3	Srikanth [24]	Brute force attacks detection on IoT networks using deep learning techniques	2021	Deep learning detected brute-force attacks on MQTT / IoT networks with very high accuracy (reported >99%)
4	Alaiz-Moretón *et al.* [1]	Multi-class classification procedure for detecting attacks on MQTT-IoT protocol	2019	Proposed and evaluated multiclass procedures addressing multiple intrusion types on MQTT
5	Rani *et al.* [19]	An ensemble-based multi-class classifier for intrusion detection using Internet of Things	2022	Proposed an ensemble multiclass classifier for IoT IDS (discussion/recommendation for multiclass setups)
6	Shirodkar [22]	Brute force attacks detection on IoT networks using deep learning techniques	2023	Reported ~99% classification accuracy distinguishing regular vs. brute-force attacks on MQTT-IoT-IDS2020
7	Churcher *et al.* [7]	An experimental analysis of attack classification using machine learning in IoT networks	2021	Reported ~99% accuracy (KNN) for multiclass attack classification (Sensors study)
8	Sarhan *et al.* [21]	NetFlow datasets for machine learning-based network intrusion detection systems	2021	Provided five labelled NIDS/NetFlow datasets for multiclass classification experiments (dataset paper)
9	Le *et al.* [12]	XGBoost for imbalanced multi-class classification-based Internet of Things intrusion detection systems	2022	Proposed XGBoost; reported very high F1 scores (e.g., 99.9% / 99.87% on X-IIoTDS and TON_IoT in the paper)
10	Tiwari *et al.* [25]	A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security	2024	Reported very high accuracy on an IIoT dataset using PSO + PCA + MARS (authors report near-perfect/very high accuracy)

Table 3. Detailed Multi-Class Classification Report using _OvO and _OvR

The _OvO. Model				The _OvR. Model				
	IoT-Fridge _Dataset (Acc = 100%)							
_sub-class	_Precision	_Recall	_F1-Score	_Support	_Precision	_Recall	_F1-score	_Support
ransomware	1.00	1.00	1.00	10558	1.00	1.00	1.00	10558
_normal	1.00	1.00	1.00	3018	1.00	1.00	1.00	3018
_ddos	1.00	1.00	1.00	2122	1.00	1.00	1.00	2122
_backdoor	1.00	1.00	1.00	150423	1.00	1.00	1.00	150423
_injection	1.00	1.00	1.00	8569	1.00	1.00	1.00	8569
_xss	1.00	1.00	1.00	840	1.00	1.00	1.00	840
_password	1.00	1.00	1.00	593	1.00	1.00	1.00	593
_Accuracy			1.00	176123			1.00	176123
_Macro-avg	1.00	1.00	1.00	176123	1.00	1.00	1.00	176123
_Weighted-avg	1.00	1.00	1.00	176123	1.00	1.00	1.00	176123
	IoT-Weather _Dataset (Acc = 99.97%) and (Acc = 98%)							
sub-class	_Precision	_Recall	_F1-Score	_Support	_Precision	_Recall	_F1-score	_Support
_xss	1.00	1.00	1.00	10692	0.90	1.00	0.95	10692
ransomware	1.00	1.00	1.00	4510	0.85	0.64	0.73	4510
_normal	1.00	1.00	1.00	2833	0.80	0.66	0.72	2833
_password	1.00	1.00	1.00	167944	1.00	1.00	1.00	167944
_ddos	1.00	1.00	1.00	7835	0.83	1.00	0.91	7835
_injection	0.96	0.99	0.98	839	0.00	0.00	0.00	839
_backdoor	1.00	1.00	0.90	162	0.00	0.00	0.00	162
_scanning	0.99	0.93	0.96	258	0.00	0.00	0.00	258
*_Accuracy_*			1.00	195073			0.98	195073
*_Macro-avg_*	0.99	0.97	0.98	195073	0.54	0.54	0.54	195073
_Weighted-avg	1.00	1.00	1.00	195073	0.97	0.98	0.98	195073
	IoT-Modbus _Dataset (Acc = 77.6158%)							
sub-class	_Precision	_Recall	_F1-Score	_Support	_Precision	_Recall	_F1-score	_Support
_xss	0.00	0.00	0.00	12015	0.00	0.00	0.00	12015
_password	0.00	0.00	0.00	1561	0.00	0.00	0.00	1561
_injection	0.78	1.00	0.87	66873	0.78	1.00	0.87	66873
_normal	0.00	0.00	0.00	5382	0.00	0.00	0.00	5382
_backdoor	0.00	0.00	0.00	178	0.00	0.00	0.00	178
_scanning	0.00	0.00	0.00	150	0.00	0.00	0.00	150
_Accuracy			0.78	86159			0.78	86159
_Macro-avg	0.13	0.17	0.15	86159	0.13	0.17	0.15	86159
_Weighted-avg	0.60	0.78	0.68	86159	0.60	0.78	0.68	86159

5. Conclusions

The importance of strong Intrusion Detection Systems (IDS) in protecting IoT settings is emphasised by this study. Multi-class classification approaches and machine learning algorithms were used in the study to handle the increasing diversity and complexity of cyber threats in IoT networks. Strong performance is shown in the findings, especially when using the IoT-Fridge and IoT-Weather datasets, which had 100% and 99.97% accuracy, respectively. The findings indicate that the proposed models are capable of identifying and classifying various types of intrusions in datasets that have different characteristics. However, the IoT-Modbus dataset that yielded a smaller accuracy of 77.6%, found some problems that should be addressed to enhance the performance of IDS systems when handling more complex datasets. The analytical findings explain why the creation of standard dataset features and sophisticated classification procedures and continuous system upgrades of IDS are essential to the current IoT security systems.

Future Works

Future research on the exploration of advanced ML models and various datasets should focus on the limitations of the study and conduct testing on real IoT data streams. Researchers ought to think of increasing the number of IoT datasets that differ in complexity and also in the type of attack and network structure. The suggested approaches would be more convenient in terms of performance assessment and the scenarios of various IoT settings could be tested. Real-time testing of IoT streams is conducted to demonstrate how the developed models are operated within operational IoT environments. Hybrid modelling techniques represent an important area of prospective research among IDS experts. A combination approach using various ML algorithms strengthens IDS systems by maximizing their performance and reliability. Complex datasets would display subtle patterns to both traditional and DL methods through the combination of CNNs or LSTM networks and classification approaches. Stacking together with bagging and boosting methodologies enables the improvement of predictive accuracy and builds model stability. To achieve successful operation of IDS systems in practical scenarios real-time processing plays a vital role. New research should study the development of progressive learning methods which enable models to change their behavior when presented with new information without requiring complete retraining processes.

Recommendations

Based on the outcomes, some recommendations are proposed to enhance IDS development. Addressing class imbalance in imbalanced datasets represents the first recommendation as it is very critical challenge in datasets like IoT-Modbus. Therefore, approaches such as *Synthetic Minority Oversampling Technique* (SMOTE), targeted sampling, or data augmentation can be utilized for balancing all classes among the used dataset (Booij and Chiscop [6]). Doing so, would improve model's ability in accurately classify the low represented classes in which it reduces the likelihood of mis-classifications. Additionally, implementing of advanced feature engineering methods can be examined for dataset quality optimization. Among the famous approaches, dimensionality reduction techniques, such as Principal Component Analysis (PCA) could assist in eliminating noise and shed light on the most relevant attributes (Kaushik and Al-Raweshidy [10], and Samita [20]). On the other hand, the automation of feature selection processes was achieved through the utilization of algorithms such as *Recursive Feature Elimination* (REF), by which the preprocessing pipeline was streamlined to enhance model efficiency. Another important aspect to be considered was hyperparameters tuning. Methods such as Bayesian optimization or grid search were employed so that the optimal settings for various datasets and classification models could be automatically determined. When adopted these approaches ensured that every model was optimized to attain the highest possible level of performance. Lastly, to ensure the reliability of performance metrics validation techniques such as k-fold cross-validation were applied. Through these techniques overfitting was effectively avoided and a more accurate understanding of the model's behavior on unseen data was obtained.

Acknowledgement

The author extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2025-1754).

Competing Interests

The author declares that he has no competing interests.

Authors' Contributions

The author wrote, read and approved the final manuscript.

References

[1] H. Alaiz-Moreton, J. Aveleira-Mata, J. Ondicol-Garcia, A. L. Muñoz-Castañeda, I. García and C. Benavides, Multiclass classification procedure for detecting attacks on MQTT-IoT protocol, *Complexity* **2019**(1) (2019), 6516253, DOI: 10.1155/2019/6516253.

[2] M. Al-Boghdady, M. El-Ramly and K. Wassif, iDetect for vulnerability detection in Internet of Things operating systems using machine learning, *Scientific Reports* **12** (2022), Article number: 17086, DOI: 10.1038/s41598-022-21325-x.

[3] B. K. Alotaibi, F. A. Khan, Y. Qawqzeh, G. Jeon and D. Camacho, Performance and communication cost of deep neural networks in federated learning environments: An empirical study, *International Journal of Interactive Multimedia and Artificial Intelligence* **9**(4) (2024), 6 – 17, DOI: 10.9781/ijimai.2024.12.001.

[4] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood and A. Anwar, TON_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems, *IEEE Access* **8** (2020), 165130 – 165150, DOI: 10.1109/ACCESS.2020.3022862.

[5] A. Azab, M. Khasawneh, S. Alrabaee, K.-K. R. Choo and M. Sarsour, Network traffic classification: Techniques, datasets, and challenges, *Digital Communications and Networks* **10**(3) (2022), 676 – 692, DOI: 10.1016/j.dcan.2022.09.009.

[6] T. Booij and I. Chiscop, Statistical analysis of ToN_IoT datasets, *IEEE DataPort* (2021), DOI: 10.21227/frw4-sk06.

[7] A. Churcher, R. Ullah, J. Ahmad, S. ur Rehman, F. Masood, M. Gogate, F. Alqahtani, B. Nour and W. J. Buchanan, An experimental analysis of attack classification using machine learning in IoT networks, *Sensors* **21**(2) (2021), 446, DOI: 10.3390/s21020446.

[8] A. Dahou, M. A. Elaziz, S. A. Chelloug, M. A. Awadallah, M. A. Al-Betar and M. A. A. Al-qaness and A. Forestiero, Intrusion detection system for IoT based on deep learning and modified reptile search algorithm, *Computational Intelligence and Neuroscience* **2022** (2022), Article ID 6473507, DOI: 10.1155/2022/6473507.

[9] O. Elnakib, E. Shaaban, M. Mahmoud and K. Emara, EIDM: Deep learning model for IoT intrusion detection systems, *The Journal of Supercomputing* **79** (2023), 13241 – 13261, DOI: 10.1007/s11227-023-05197-0.

[10] A. Kaushik and H. Al-Raweshidy, A novel intrusion detection system for Internet of Things devices and data, *Wireless Networks* **30** (2024), 285 – 294, DOI: 10.1007/s11276-023-03435-0.

[11] F. A. Khan, A. Rahman, M. Alharbi and Y. K. Qawqzeh, Awareness and willingness to use PHR: A roadmap towards cloud-dew architecture based PHR framework, *Multimedia Tools and Applications* **79** (2020), 8399 – 8413, DOI: 10.1007/s11042-018-6692-z.

[12] T.-T.-H. Le, Y. E. Oktian and H. Kim, XGBoost for imbalanced multi-class classification-based Internet of Things intrusion detection systems, *Sustainability* **14**(14) (2022), 8707, DOI: 10.3390/su14148707.

[13] R. Priya, N. Suman, A. Utsav and A. Abhishek, Internet of Things (IoTs) - Review and it's multiple classification, in: *Proceedings of the Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks* (ICICV, Tirunelveli, India, 2021), pp. 328 – 334 (2021), DOI: 10.1109/ICICV50876.2021.9388464.

[14] R. Qaddoura, A. M. Al-Zoubi, H. Faris and I. Almomani, A multi-layer classification approach for intrusion detection in IoT networks based on deep learning, *Sensors* **21**(9) (2021), 2987, DOI: 10.3390/s21092987.

[15] Y. K. Qawqzeh and M. Ashraf, A fraud detection system using decision tree classification in online transactions, in: *Proceedings of the 12th International Conference on Software and Computer Applications* (ICSCA 2023, Kuantan, Malaysia, 2023), pp. 1 – 8 (2023), DOI: 10.1145/3587828.3587860.

[16] Y. Qawqzeh and W. Samaraa, Deep learning-based multiclass anomaly detection in the IoT_GPS_Tracker dataset: Unveiling patterns for enhanced tracking accuracy, in: *Proceedings of the 2023 International Conference on Advances in Computation, Communication and Information Technology* (ICAICCIT, Faridabad, India, 2023), pp. 687 – 690 (2023), DOI: 10.1109/ICAICCIT60255.2023.10466099.

[17] Y. K. Qawqzeh, A. Alourani and S. Ghwanmeh, An improved breast cancer classification method using an enhanced AdaBoost classifier, *International Journal of Advanced Computer Science and Applications* **14**(1) (2023), 473 – 478, DOI: 10.14569/IJACSA.2023.0140151.

[18] Y. Qawqzeh, M. B. I. Reaz, M. A. M. Ali, K. B. Gan, S. Zulkifli and A. Noraidatulakma, Assessment of atherosclerosis in erectile dysfunction subjects using second derivative of photoplethysmogram, *Scientific Research and Essays* **7**(25) (2012), 2230 – 2236, URL: https://academicjournals.org/journal/SRE/article-abstract/898213227600.

[19] D. Rani, N. S. Gill, P. Gulia and J. M. Chatterjee, An ensemble-based multiclass classifier for intrusion detection using Internet of Things, *Computational Intelligence and Neuroscience* **2022** (2022), Article ID 1668676, DOI: 10.1155/2022/1668676.

[20] Samita, A review on intrusion detection systems for IoT-based systems, *SN Computer Science* **5** (2024), article number 380, DOI: 10.1007/s42979-024-02702-x.

[21] M. Sarhan, S. Layeghy, N. Moustafa and M. Portmann, NetFlow datasets for machine learning-based network intrusion detection systems, in: *Big Data Technologies and Applications*, Z. Deze, H. Huang, R. Hou, S. Rho and N. Chilamkurti (editors), (BDTA WiCON 2020), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 371, Springer, Cham., pp. 117–135 (2021), DOI: 10.1007/978-3-030-72802-1_9.

[22] S. A. Shirodkar, Brute force attacks detection on IoT networks using deep learning techniques, *International Journal of Advanced Research in Science, Communication and Technology* **3**(3) (2023), 599 – 605, DOI: 10.48175/IJARSCT-11493.

[23] R. Singh and R. L. Ujjwal, A comprehensive review of IoT-based IDS using intelligence technique, in: *Advances in Data and Information Sciences* (Lecture Notes in Networks and Systems, vol. 522), S. Tiwari, M. C. Trivedi, M. L. Kolhe and B. K. Singh (editors), Springer, Singapore (2023), DOI: 10.1007/978-981-19-5292-0_11.

[24] P. Srikanth, An efficient approach for clustering and classification for fraud detection using bankruptcy data in IoT environment, *International Journal of Information Technology* **13**(6) (2021), 2497 – 2503, DOI: 10.1007/s41870-021-00756-1.

[25] R. S. Tiwari, D. Lakshmi, T. K. Das, A. K. Tripathy and K.-C. Li, A lightweight optimized intrusion detection system using machine learning for edge-based IIoT security, *Telecommunication Systems* **87** (2024), 605 – 624, DOI: 10.1007/s11235-024-01200-y.

[26] S. Ullah, J. Ahmad, M. A. Khan, E. H. Alkhammash, M. Hadjouni, Y. Y. Ghadi, F. Saeed, and N. Pitropakis, A new intrusion detection system for the Internet of Things via deep convolutional neural network and feature engineering, *Sensors* **22**(10) (2022), 3607, DOI: 10.3390/s22103607.

[27] A. Vardhan, P. Kumar and L. K. Awasthi, A resilient intrusion detection system for IoT environment based on a modified stacking ensemble classifier, *SN Computer Science* **5** (2024), article number 1020, DOI: 10.1007/s42979-024-03364-5.

[28] S. Yaras and M. Dener, IoT-based intrusion detection system using a new hybrid deep learning algorithm, *Electronics* **13**(6) (2024), 1053, DOI: 10.3390/electronics13061053.