ISSN: 2584-0495 Vol. 3, Issue 5, pp. 1656-1662

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

Active Learning and Label Spreading Semi-Supervised Learning Techniques for Detection of Firewall Actions

Diksha, Shweta Sharma, Sweeti Sah, Vijay Nath

Cite as: Diksha, Sharma, S., Sah, S., & Nath, V. (2025). Active Learning and Label Spreading Semi-Supervised Learning Techniques for Detection of Firewall Actions. International Journal of Microsystems and IoT, 3(5), 1656–1662. https://doi.org/10.5281/zenodo.18152466

Published online: 20 May 2025

https://doi.org/10.5281/zenodo.18152466

International Journal of Microsystems and IoT
Vol.3, Issue 5, pp.1656-1662; DOI: https://doi.org/10.5281/zenodo.18152466

Active Learning and Label Spreading Semi-Supervised Learning Techniques for Detection of Firewall Actions

Diksha[1], Shweta Sharma[1], Sweeti Sah[1], Vijay Nath[2]

[1]Department of Computer Engineering, National Institute of Technology Kurukshetra, Haryana, India
[2]Department of Electronics & Communication Engineering, Birla Institute of Technology Mesra, Ranchi, Jharkhand, India

ABSTRACT
Firewalls are essential for network security because they sort incoming traffic into several categories such as accept, deny, or drop/reset. Existing classification techniques are based on supervised learning techniques in which manual labelling on complete dataset is required. In this experimental work, we are using semi-supervised learning using the Internet Firewall-2019 dataset which contains extensive numbers and types of actual firewall log records. The proposed framework has two algorithms which are the Label Spreading that propagates labels through graphs between data points of similar attributes. In addition, it introduces a new active learning algorithm which was proposed to deal with the following kinds of problems: the reduction of false positives and threat packets received automatically in time-efficient manner. The two methods have been demonstrated to be useful in the categorizing firewall operations in experimental evaluation. Active Learning technique can be characterized by outstanding accuracy. It detects with high accuracy of 99.80% which is impressive and adaptive for cybersecurity future use.

KEYWORDS
Firewall; Machine Learning; Active Learning; Label Spreading; Semi-supervised

1. INTRODUCTION

Modern networks are becoming more vulnerable to network attack known as man in the middle attack because of the increasing trend of reliance on the digital communication systems and wide range of security-related breaches and cyber-attacks. When unauthorized access is achieved, malicious actors will be able to take data outtake sensitive information or manipulate data integrity during the lifecycle of a network. Consequently, the network infrastructures have been subjected to multi-level security frameworks, which are used to identify, resist, and react even against such threats. These include firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) as some of the critical elements in the protection profile of information systems.

Firewalls especially are the major defense between secure internal systems and untrusted outside parties. They are commonly placed at the border of networks and determine the traffic flow by examining packets and act according to the set policies. Decisions made by these (routinely classified as allow, deny, or drop/reset) are recorded in detail, are called firewall logs. Through the analysis of these logs, insights into the traffic behavior are obtained, and such information is useful in the establishment of patterns attributed to malicious activity. Machine Learning (ML) methodologies have become popular in order to make the firewall systems more responsive and intelligent since they represent the complex signal processing and allow automatizing the classification process. ML provides adaptive systems, which can learn from the historical information to predict the right course of action by the firewall against the new instances of the traffic.

Such a combination of cybersecurity and artificial intelligence has seen the growth of more innovative solutions with high accuracy rates in detection and fewer instances of manual supervision.

Well-known models used in cybersecurity are Artificial Neural Networks (ANN), Support Vector Machines (SVM), Decision Trees, K-Nearest Neighbors (KNN), Convolutional Neural Networks (CNN) [23], and different forms of ensemble. The motivation behind the efficiency of these algorithms has to do with the nature of the data in terms of dimensions, its distribution, and labeling quality. Within this work, we use the publicly available Internet Firewall-2019 (IFW-2019) dataset [20] as the base of our research, the aim of which is to provide evidence that supports the idea that two novel machine learning methods are effective in terms of firewall action detection: Label Spreading [1] and Active Learning [2]. They both seek to enhance the automation and precision of firewall decision-making under the conditions of scarce labeled data, improving the advancement of smarter and more effective network protection data formations.

1.1. Contributions

This research work has made key contributions highlighted as follows:

- **Active Learning of Threat Detection in Firewall:** To the best of our knowledge, this is the first experimental study to apply active learning in the domain of firewall action classification. A novel semi-supervised [24] Active Learning algorithm [25] is proposed to reduce the time required in labeling and yet to increase the accuracy. This enables it to minimize false positives, and improves on threat detection because only the unsure samples are

queried.

- **Label Spreading of Threat Detection in Firewall:** This is the first work that demonstrates the efficiency of label spreading (a semi-supervised learning algorithm) in firewall threat detection using real-world firewall datasets**.** Label Spreading is used as a graph based approach to label firewall actions where only a few labeled data is available and performs well in semi-supervised setting.

2. LITERATURE SURVEY

In the corresponding research, Ertam [3] suggested a new data classification method to interact with firewalls based on deep learning. Ten cases are analyzed to come up with numerical results. The framework includes the following steps: data retrieving on the firewall, feature selection and classification. A range of different classifiers, including Long Short-Term Memory (LSTM), Bi-directional LSTM and SVM were used by the author to evaluate the model. They therefore concluded that the Bi-LSTM-LSTM deep learning-based hybrid network is better than the SVM classifier since it recorded highest accuracy of 97.38%. To conclude, they noted that smart monitoring system is very effective way of solving security of networks.

Moreover, the use of Reinforcement Learning (RL) methods was observed in this field because the current study carried out by J. Jeya Prasad *et al.* [4] employed it successfully. In this research RL based and pattern matching (PM) firewall that is used in secured cloud infrastructure. The firewall will avoid malicious attacks by ensuring that the signature of the payload of the incoming packets is verified. The hybrid system model they came up with provides a pattern matching algorithm which verifies the signature so that to simplify the fast decision-making process. The simulation results depicted that their proposed RLPM model showed a 10 percent decline in the firewall response time, throughput and Malevolent attack blocking, relative to the existing state-of-the-arts systems.

In another model of firewall classification, the classification model presented by Al-Haijaa & Ishtaiwi [5] uses Shallow Neural Networks (SNN) and Optimizable Decision Trees (ODT). They achieved accuracies of 99.8% and 98.5% with SNN and ODT in the IFW-2019 dataset respectively. Shaheed & Kurdy [6] developed a framework using ML and feature engineering of web attacks. Request length, the percentages of special characters among others were also extracted and grouped using algorithms like the Naive Bayes and SVM. Their method achieved an accuracy of 99.6% on research data and 98.8% on real world logs.

Liang *et al.* [7] presented GPTFuzzer, a technique for evaluating Web Application Firewalls (WAFs) via a Generative Pre-trained Transformer (GPT) model. It surpassed state-of-the-art techniques, detecting up to 7.8 additional bypassing payloads or necessitating an average of 8.1 fewer requests. Nevertheless, it had a restricted emphasis on the practical ramifications of the identified bypassing payloads in real-world contexts. Maiga *et al.* [8] presented a human-machine design to mitigate false alarms in intrusion detection systems (IDS) by probabilistic clustering. Network traffic is categorized according to the probabilities generated by a deep learning algorithm, with identified clusters directed to human specialists for evaluation. The incorporation of a next-generation firewall (NGFW) into the architecture enhanced traffic processing efficiency. In benchmark datasets (CICDDoS2019, UNSW-NB15, CICIDS2017), their hybrid CNN-RNN model diminished false positives by 79.61% and false negatives by 86.99%.

Karunakaran *et al* [9] (2024) developed a blockchain-based access control system for IIoT security, integrating an attribute-based access control engine with an AI classifier. A CNN analyzes IoT traffic to classify transactions as legitimate or malicious, while blockchain records key decisions for transparency and resilience. Tested on the TON_IoT dataset, the system achieved a 99.26% accuracy in detecting malicious activity, offering a scalable and accountable approach to IIoT security.

Similarly, Uçar *et al*. [10] presented a machine learning method to detect anomalies in firewall rule sets, evaluating several classifiers on firewall logs. The kNN classifier performed best, with an F-Measure of 93%, demonstrating the effectiveness of ML in identifying irregularities within firewall configurations.

Additionally, several other prospective state-of-the-art studies have been conducted in the field of cybersecurity using deep neural networks [11]– [21].

2.1 Research Gaps

In the existing literature, researchers have primarily employed supervised and unsupervised machine learning algorithms for firewall threat detection. Supervised learning methods, while generally accurate, require extensive manual labeling, which is both time-consuming and prone to human error. On the other hand, unsupervised learning techniques eliminate the need for labeled data but often suffer from lower accuracy due to the absence of guided training signals.

To address these limitations, this experimental work proposes the application of semi-supervised machine learning techniques, specifically Active Learning and Label Spreading. These approaches strike a balance between the need for labeled data and model performance. By leveraging a small amount of labeled data alongside a large pool of unlabeled samples, semi-supervised learning significantly reduces labeling effort while improving detection accuracy. This work fills the research gap by demonstrating the effectiveness of semi-supervised methods in real-time firewall action classification.

3. DATASET OVERVIEW

In this section, the publicly available IFW-2019 [16] dataset, which contains a total of 65,532 records collected from real-world firewall logs. Each record corresponds to a network event processed by a firewall system, with the associated action categorized into one of four classes: allow, deny, drop, or reset-both. These labels reflect the firewall's response to incoming traffic—either permitting it, blocking it, silently discarding it, or resetting the connection for both ends. The distribution of records across the four action classes is summarized below in Table 1.

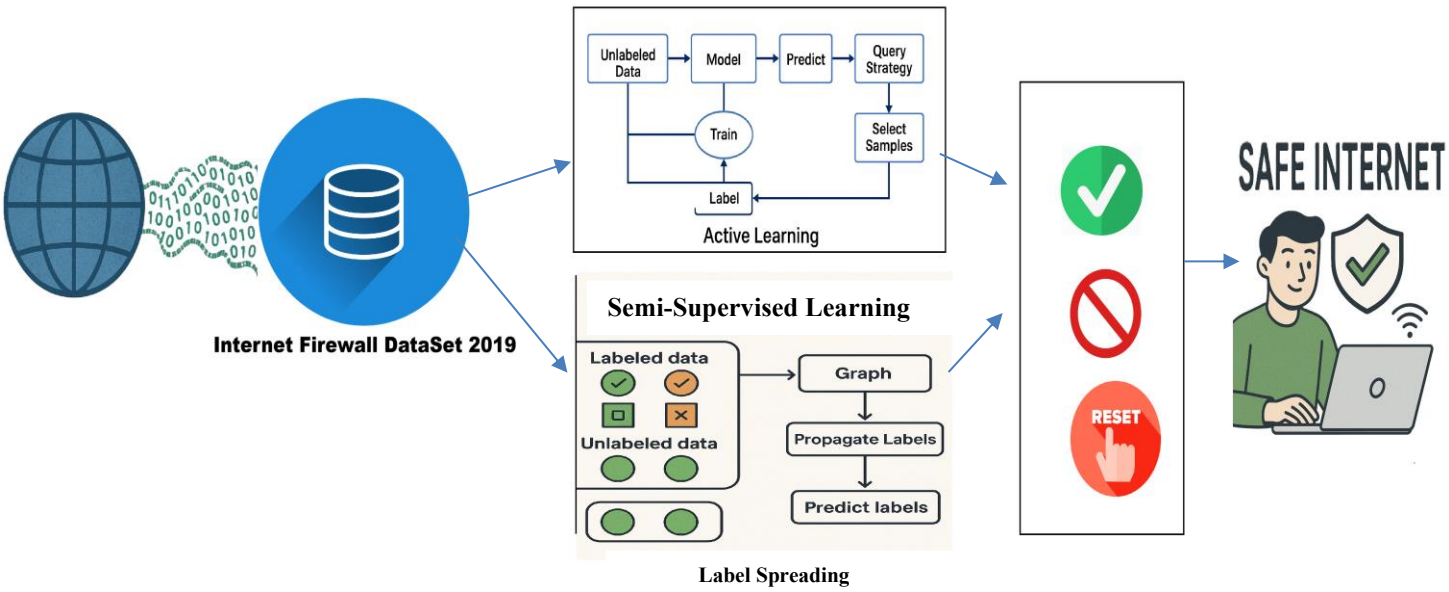


Figure 1 Architecture of Proposed Framework

Table 1 Statistics of Traffic Distribution for IFW-2019 Dataset

Action	Number of Records	Description
Allow	37,640	Packet is permitted through the firewall
Deny	14,987	Packet is explicitly blocked
Drop	12,851	Packet is silently dropped without notification
Reset-both	54	TCP connection is forcefully reset for both endpoints

The categorical datatype in which the dataset class features are recorded must be encoded into numerical labels (labelling) in order to be processed mathematically by the machine learning algorithms and calculations. In order to ensure that the target classes are appropriately labelled, we have implemented the single hot encoding technique as follows: Allow (0), Deny (1), Drop (2), and Reset (3).

4. PROPOSED SEMI-SUPERVISED LEARNING TECHNIQUES FOR DETECTION OF FIREWALL ACTIONS

In this experimental work, we constructed a classification system utilizing a Label Spreading method and active learning to train and categorize the communication traffic records from the IFW-2019 dataset into three classifications: Allow, Deny, Drop and Reset. The architecture of proposed framework is described in Figure 1, in which label spreading and active learning semi-supervised algorithms are used. These algorithms are explained as follows:

4.1 **Label Spreading Semi-Supervised Technique:** The Label Spreading algorithm is a graph-based semi-supervised learning technique that propagates label information from a small set of labeled data points to a larger set of unlabeled data points [1]. By leveraging the structure of the data distribution, Label Spreading iteratively spreads label information across the dataset, ensuring that similar data points are assigned the same or similar labels. The proposed Label Spreading algorithm ensures that the label information is propagated smoothly across the dataset, leveraging the underlying data structure to improve classification performance.

Algorithm 1 Label Spreading Algorithm

1: Input: Dataset with labeled and unlabeled samples, parameter α, kernel type (e.g., 'knn' or 'rbf')
2: Output: Predicted labels for unlabeled samples
3: Data Preprocessing
4: Dataset Splitting: Divide the dataset into:
Labeled data: Known labels for initial supervision
Unlabeled data: Labels to be inferred
5: Graph Construction
Construct a similarity graph using RBF kernel:
$w_{ij} = \exp(-\|x_i - x_j\|^2 / 2\gamma^2)$
where γ controls the sensitivity of similarity
6: Label Propagation :Initialize label matrix Y (known labels for labeled data, zeros for unlabeled)
7.: Iteratively update label distribution F using:
$F = \alpha W F + (1 - \alpha)Y$
W is the normalized similarity matrix
8: Convergence and Prediction
9: Repeat until F converges (labels stabilize)
10: Assign final labels to unlabeled data based on the maximum value in each row of F
11: return Final predicted labels

4.2 **Active Learning Semi-Supervised Technique:** The proposed Active Learning algorithm is an iterative learning technique designed to improve the performance of a machine learning model by intelligently selecting the most informative samples from an unlabeled dataset for labelling [2]. By focusing on the most uncertain or diverse samples, Active Learning minimizes the labeling effort while maximizing the model's performance. The proposed

Active Learning algorithm ensures efficient utilization of labelling resources while improving the model's performance iteratively. By focusing on the most informative samples, the algorithm reduces the labelling effort required to achieve high classification accuracy.

Algorithm 2 Active Learning Algorithm

1: Input: Labeled dataset (Xlabeled, ylabeled), Unlabeled dataset Xunlabeled,Query size n, Strategy type (e.g., entropy, margin, least confident)
2: Output: Updated labeled dataset (Xcombined, ycombined)
3: Data Preprocessing
4: Model Initialization: Train a Random Forest Classifier on Xlabeled
5: Predict probability distributions for Xunlabeled
6: if strategy == 'entropy' then
    Compute uncertainty as − P p log(p) (high entropy indicates uncertainty)
7: else if strategy == 'margin' then
    Compute margin as difference between top two class probabilities (lower margin implies uncertainty)
8: else if strategy == 'least confident' then
    Compute uncertainty as 1 − max(p) (lowest confidence indicates uncertainty)
9: else
    Raise error for invalid strategy
10: end if
11: Query Selection
12: Select n most uncertain samples from $X_{unlabeled}$
13: Labeling
14: Predict labels for selected samples (or receive from annotator)
15: Dataset Update
16: Combine selected samples and their labels with $X_{labeled}$ and $y_{labeled}$ to form $X_{combined}$ and $y_{combined}$
17: return $X_{combined}$, $y_{combined}$

The proposed methodology employs two core algorithms for semi-supervised firewall action classification. **Algorithm 1** outlines the use of Label Spreading, where label propagation is conducted over a similarity graph using iterative matrix updates. This technique efficiently infers labels for large amounts of unlabeled data. Following this, **Algorithm 2** describes an Active Learning strategy that incrementally selects the most uncertain samples using entropy or margin-based uncertainty, minimizing annotation cost while improving classification performance.

5. RESULT AND DISCUSSION

This section presents and compares the result of two semi-supervised learning methodologies—Active Learning employing entropy-based sampling and Label Spreading—applied to the classification of intelligent firewall actions utilizing the IFW-2019 dataset.

5.1. Experimental Result

The result shows that Active Learning model achieved excellent classification performance. After querying 1,000 most uncertain samples (based on entropy) and retraining the model. The confusion matrix of Active Learning is described in Figure 2.

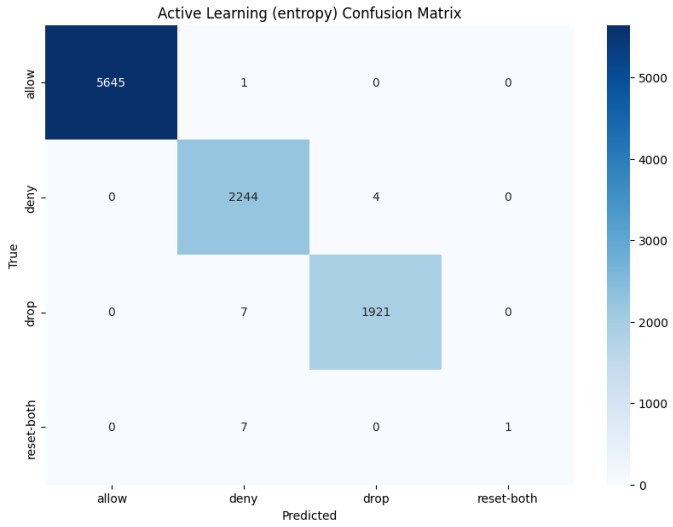


Figure 2 Confusion Matrix for Active Learning

Label Spreading model was trained with 20% of the samples labeled, while the remaining 80% were considered unlabeled. The findings indicated that the algorithm successfully learned distinguishing patterns and accurately assigned class labels to the unlabeled data. The model achieved an overall accuracy of 94.55% on the inferred data, demonstrating commendable efficacy for semi-supervised classification in the cybersecurity sector. The confusion matrix of label spreading is described in Figure 3.

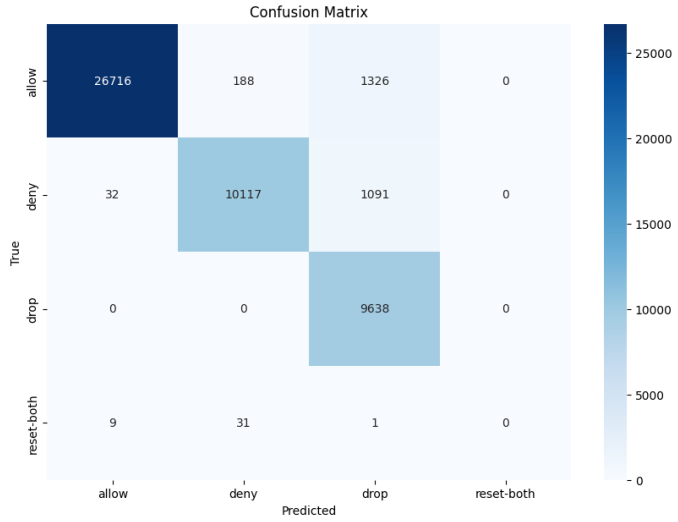


Figure 3 Confusion Matrix for Label Spreading

The comparison of experimental work is described in Table 2. Active Learning attains superior accuracy by selectively querying the most informative and uncertain examples from the pool of unlabeled data for annotation. This technique guarantees that the model is perpetually trained on the most difficult and boundary-defining examples, thus enhancing its generalization capability. Active Learning mitigates redundancy and emphasizes essential decision boundaries, thereby diminishing classification ambiguity and improving detection accuracy in firewall threat classification tasks.

Table 2 Performance Comparison of Proposed Models

Metric	Active Learning	Label Spreading
Accuracy	99.806%	94.551%
Precision	99.807%	95.411%
Recall	99.806%	94.551%
F1-Score	99.779%	94.684%

The ROC curves for all classes show near-perfect AUC scores of 1.00, indicating the model's robustness in separating the different firewall actions. The ROC curve is described in Figure 4.

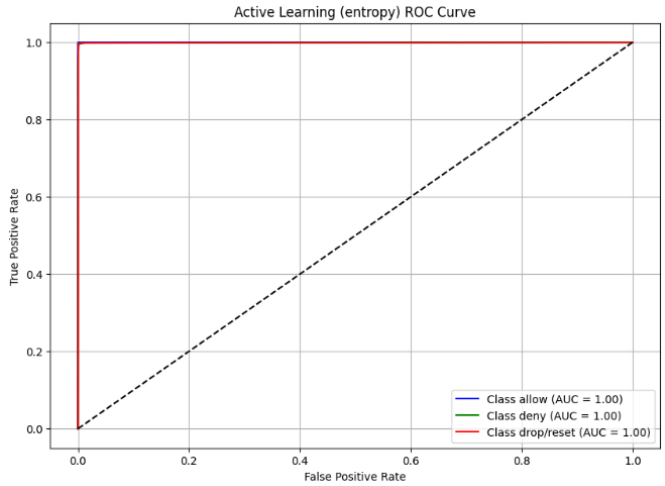


Figure 4 ROC Curve for Active Learning

5.2. Comparison with Existing work

Figure 5 illustrates a comparative analysis between the proposed framework and several state-of-the-art models for firewall traffic classification. The comparison shows that the proposed framework achieve best accuracy as compared to the existing frameworks.

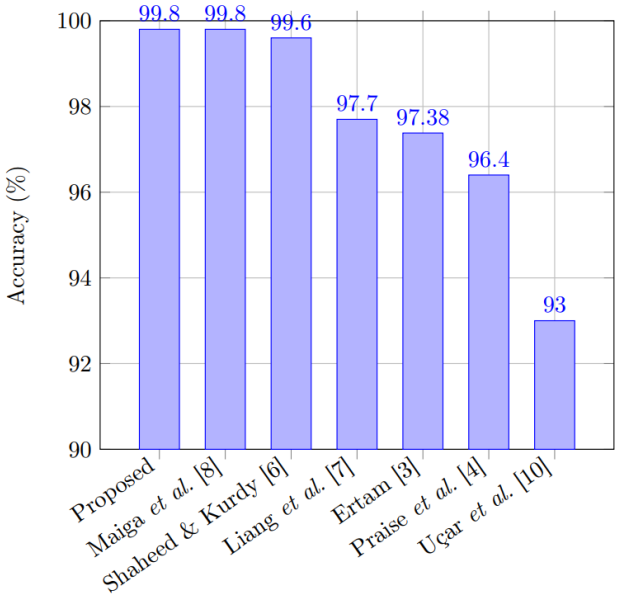


Figure 5 Comparison with Existing work

6. CONCLUSION AND FUTURE SCOPE

This research investigated two robust semi-supervised learning methodologies—Active Learning (utilizing entropy-based sampling) and Label Spreading—to effectively categorize firewall operations employing the IFW-2019 dataset. Both methodologies sought to utilize the plentiful unlabeled data while reducing manual annotation requirements, which is particularly advantageous in practical cybersecurity applications. The Active Learning approach, especially with entropy-based sampling, shown remarkable efficacy with an accuracy of 99.80%, proficiently discerning essential firewall

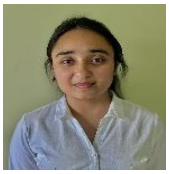
actions like allow, deny, and the combination drop/reset. Its capacity to iteratively enhance the model by choosing the most informative samples renders it an exceptionally efficient solution for dynamic and adaptive threat detection contexts. Conversely, the Label Spreading algorithm, while promising, attained a lower accuracy of 94.55% and encountered difficulties with underrepresented classes such as reset-both. It continues to be an effective approach for bootstrapping models with limited supervision, especially when class distribution is relatively balanced.

In future work, we can integrate resampling techniques, synthetic data creation (e.g., SMOTE), or cost-sensitive learning to alleviate performance decline on infrequent yet significant classes such as reset-both.

REFERENCES

1. M. Fan, X. Zhang, L. Du, L. Chen, D. Tao, Semi-supervised learning through label propagation on geodesics, IEEE Transactions on Cybernetics 48 (2018) 1486–1499
2. X. Chen, T. Wang, Combining active learning and semi-supervised learning by using selective label spreading, in: 2017 IEEE International Conference on Data Mining Workshops (ICDMW), 2017, pp. 850–857
3. F. Ertam, "An efficient hybrid deep learning approach for internet security", Physica A: Statistical Mechanics and its Applications, Elsevier, vol. 535, 2019
4. J.J. Praise, R.J Raj, J.V. Benifa, "Development of Reinforcement Learning and Pattern Matching (RLPM) Based Firewall for Secured Cloud Infrastructure", Wireless Personal Communication, Springer, vol.115, pp. 993–1018, 2020
5. Q. A. Al-Haijaa and A. Ishtaiwi, "Machine Learning Based Model to Identify Firewall Decisions," International Journal on Advanced Science Engineering and Information Technology, vol. 11, pp. 1688-1695, 2021
6. M. Kurdy and A. Shaheed, "Web Application Firewall Using Machine Learning and Features Engineering" Security and Communication Networks, Wiley, vol. 2022, pp.1-14, 2022
7. H. Liang, X. Li, D. Xiao, J. Liu, Y. Zhou, A. Wang, J. Li, Generative pre-trained transformer-based reinforcement learning for testing web application firewalls, IEEE Transactions on Dependable and Secure Computing 21 (2023) 309–324
8. A. A. Maiga, E. Ataro, and S. Githinji, "Intrusion Detection With Deep Learning Classifiers: A Synergistic Approach of Probabilistic Clustering and Human Expertise to Reduce False Alarms," IEEE Access, vol. 12, pp. 17836-17858, 2024
9. A. Hussein, M. Abdel-Basset, F. Hussain, N. I. Ghali, and A. E. Hassanien, "A novel transformer-based deep learning model for smart firewall," Journal of Big Data, Springer, vol. 11, pp. 1–27, 2024. doi: 10.1186/s40537-024-00994-7
10. E. Ucar and E. Ozhan, "The analysis of firewall policy through machine learning and data mining," Wireless Personal Communications, Springer, vol. 96, no. 2, pp. 2891–2909, 2017
11. G. Bendiab, S. Shiaeles, A. Alruban, N. Kolokotronis, "IoT Malware Network Traffic Classification using Visual Representation and Deep Learning", in Proc. of 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 444–449
12. R. Shire, S. Shiaeles, K. Bendiab, B. Ghita, N. Kolokotronis, "Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualization", in Proc. Of Internet of Things, Smart Spaces, and Next Generation Networks and Systems. Lecture Notes in Computer Science; Springer, vol.11660, 2019
13. I. Baptista, S. Shiaeles, N. Kolokotronis, "A Novel Malware Detection System Based On Machine Learning and Binary Visualization", in Proc. Of IEEE International Conference on Communications (IEEE ICC), China, pp. 1–6, 2019
14. K.A. Taher, B.M. Jisan, M.M Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection", in Proc. Of International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), South Asia, 10–12 January 2019; pp. 643–646
15. X. Gao, C. Shan, C. Hu, Z. Niu, Z. Liu, "An Adaptive Ensemble Machine Learning Model for Intrusion Detection", IEEE Access, vol. 7, p.p. 82512–82521, 2019
16. Q. A. Al-Haija, M. Alkhatib, A. B. Jaafar, "Choices on Designing Gf (P) Elliptic Curve Coprocessor Benefiting from Mapping Homogeneous Curves in Parallel Multiplications", International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397, vol. 3 no. 2, 2011
17. S. Sapre, P. Ahmadi, K. Islam, "A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets through Various Machine Learning Algorithms", arXiv:1912.13204v1, 2019
18. M.M. Chowdhury, F. Hammond, G. Konowicz, C. Xin, H. Wu, J. Li, "A few-shot deep learning approach for improved intrusion detection", 2017 in Proc. Of IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), NY, USA, 19–21 October 2017; pp. 456–462
19. A. Javaid, Q. Niyaz, W. Sun, M. Alam, "A Deep Learning Approach for Network Intrusion Detection System", in Proc. of 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), NY, USA, 24 May 2016; pp. 21 26
20. Y. Imamverdiyev, L. Sukhostat, "Anomaly detection in network traffic using extreme learning machine", in Proc. of IEEE 10th International Conference on Application of Information and Communication Technologies (AICT), Azerbaijan, 12–14 October 2016; pp. 1–4
21. Q. A. Al-Haija, M. Smadi, S. Zein-Sabatto, "Multi-Class Weather Classification Using ResNet-18 CNN for Autonomous IoT and CPS Applications" in Proc. of IEEE 7th Annual Conference on Computational Science & Computational Intelligence (CSCI'20), Las Vegas, USA, 2020
22. UCI: Machine Learning Repository, "Internet Firewall Data Set", Center for Machine Learning and Intelligent Systems, 2019
23. Jablaoui, R. and Liouane, N., Network security based combined CNN-RNN models for IoT intrusion detection system. Peer-to-Peer Networking and Applications, Springer, vol. 18, pp. 1-23, 2025
24. Uthradevi, G., Thiruvasagam, P., Mythili, S. and Manoj, S.O., 2025. A Semi-Supervised Deep Learning Approach for Intrusion Detection and Classification for the Internet of Things. Biomedical Materials & Devices, pp.1-17
25. He, G., Li, B., Wang, H. and Jiang, W., 2020. Cost-effective active semi-supervised learning on multivariate time series data with crowds. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(3), pp.1437-1450

AUTHORS



Diksha received her BTech degree from Guru Jambheshwar University, Hisar, Haryana, India in 2023 and currently pursuing MTech degree in Computer Engineering (Cyber Security) from National Institute of Technology Kurukshetra, Haryana, India. Her areas of interest are network security and machine learning.

E-mail: 323103204@nitkkr.ac.in

Dr. Shweta Sharma is working as an Assistant Professor in the Dept. of Computer Engineering, National Institute of Technology Kurukshetra, Haryana, India. Her areas of interest are Cyber Security, Malware Analysis, Malware Detection, Phishing Detection, IoT, Applications of Machine and Deep Learning

E-mail: shweta.sharma@nitkkr.ac.in

Dr. Sweeti Sah is working as an Assistant Professor in the Dept. of Computer Engineering Assistant Professor, National Institute of Technology Kurukshetra, Haryana, India. Her areas of interest are Machine Learning, Deep Learning, Bioinformatics, Blockchain, Software Engineering and Image Processing.

E-mail: sweetisah3@nitkkr.ac.in

Dr. Vijay Nath is working as an Associate Professor in the Dept. of Electronics and Communication Engineering, Birla Institute of Technology. His areas of interest are VLSI, Deep Learning, and Computer Vision.

E-mail: vijaynath@bitmesra.ac.in