Mehran University Research Journal of Engineering and Technology

https://doi.org/10.22581/muet1982.2401.2945

2024, 43(1) 182-191

A novel approach to intrusion detection using zero-shot learning hybrid partial labels

Syed Atir Raza [a, *], Mehwish Shaikh [b], Raybal Akhtar [c], Aqsa Anwar [d]

[a] *School of Information Technology, Minhaj University Lahore, 54000 Pakistan*

[b] *Department of Software Engineering, Mehran University of Engineering and Technology, Jamshoro Pakistan*

[c] *School of Systems and Technology, University of Management and Technology, Lahore, 54000 Pakistan*

[d] *School of Software Engineering, Minhaj University Lahore, 54000 Pakistan*

[*] Corresponding author: Syed Atir Raza, Email: atirraza.it@mul.edu.pk

Received: 01 August 2023, Accepted: 20 December 2023, Published: 01 January 2024

K E Y W O R D S

Zero Shot Learning

Hybrid Partial Labels

Network Intrusion Detection

Network Security

A B S T R A C T

Computer networks have become the backbone of our interconnected world in today's technologically driven landscape. Unauthorized access or malicious activity carried out by threat actors to acquire control of network resources, exploit vulnerabilities, or undermine system integrity are examples of network intrusion. ZSL(Zero-Shot Learning) is a machine learning paradigm that addresses the problem of detecting and categorizing objects or concepts that were not present in the training data. . Traditional supervised learning algorithms for intrusion detection frequently struggle with insufficient labeled data and may struggle to adapt to unexpected assault patterns. In this article We have proposed a unique zero-shot learning hybrid partial label model suited to a large image-based network intrusion dataset to overcome these difficulties. The core contribution of this study is the creation and successful implementation of a novel zero-shot learning hybrid partial label model for network intrusion detection, which has a remarkable accuracy of 99.12%. The suggested system lays the groundwork for future study into other feature selection techniques and the performance of other machine learning classifiers on larger datasets. Such research can advance the state-of-the-art in intrusion detection and improve our ability to detect and prevent the network attacks. We hope that our research will spur additional research and innovation in this critical area of cybersecurity.

1. Introduction

Computer networks have become the backbone of our interconnected world in today's technologically driven landscape [1, 2]. Organizations across multiple sectors rely significantly on networked environments to support smooth communication, information sharing, and business operations, from vital infrastructure to financial systems [3, 4]. However, with greater reliance on networks comes the ever-present fear of network infiltration [5], which can interrupt services, compromise sensitive data, and result in major financial losses [6, 7].

Unauthorized access or malicious activity carried out by threat actors [8, 9] to acquire control of network resources [10], exploit vulnerabilities [11, 12], or undermine system integrity are examples of network intrusion [13, 14]. As cyber-attacks grow in sophistication and size, the requirement for powerful network intrusion detection systems (NIDS) to protect the integrity and security of these critical digital infrastructures has become critical [15, 16]. Data breaches [17], service disruptions, and the costs associated with recovery and remediation activities can all result in significant financial losses for enterprises [6]. Furthermore, intangible expenses such as brand reputation and customer trust can have far-reaching effects that go beyond direct financial consequences [18, 19].

ZSL(Zero-Shot Learning) [20] is a machine learning paradigm that addresses the problem of detecting and categorizing objects or concepts that were not present in the training data [21, 22]. Traditional machine learning algorithms require labelled training data for all conceivable classes, making generalization to previously unknown categories unfeasible [23, 24]. ZSL, on the other hand, bridges the gap between seen and unseen classes by using supplemental information such as semantic embedding [25], traits [26], or textual descriptions [27].

1.1 Motivation

It is impossible to overestimate the importance of network intrusion detection in protecting digital infrastructures from cyber threats. Traditional supervised learning algorithms for intrusion detection frequently struggle with insufficient labeled data and may struggle to adapt to unexpected assault patterns. We propose a unique zero-shot learning hybrid partial label model suited to an image-based network intrusion dataset to overcome these difficulties. Our strategy attempts to improve the accuracy, resilience, and adaptability of intrusion detection systems by leveraging zero-shot learning's capacity to distinguish new intrusion types and employing partial label techniques to handle limited labeled data. This research aims to develop intrusion detection systems, resulting in a more proactive and effective protection against the ever-changing panorama of cyber threats.

1.2 Contribution

The core contribution of this study is the creation and successful implementation of a novel zero-shot learning hybrid partial label model for network intrusion detection, which has a remarkable accuracy of 99.12%. Unlike traditional supervised learning systems, which rely largely on properly labeled data, our model uses the potential of zero-shot learning to effectively recognize and manage previously undiscovered intrusion types. This distinguishing feature is especially important in the ever-changing arena of cyber threats, as new attack patterns emerge on a regular basis. Furthermore, we incorporate partial label approaches to solve the problem of limited labeled data, which is typical in intrusion detection applications. This method allows the model to learn on partially labeled data, minimizing the cost of gathering exhaustive annotations while maintaining detection performance. Our approach's excellent accuracy supports its effectiveness and highlights its potential for real-world deployment, where fast detection and mitigation of network intrusion situations is critical.

2. State of The Art

The ever-changing geography of the malware ecosystem, along with the resource-constrained nature of current computer settings, presents severe obstacles in detecting and classifying intrusion attempts [1]. Researchers have made tremendous progress in developing various machine learning algorithms [28], such as supervised learning [29], unsupervised learning [30], and semi-supervised learning [31], to handle this complexity. These approaches strive to give intrusion detection systems the capacity to identify and categorize various intrusion events proactively. These improvements, by leveraging the power of machine learning, contribute to the establishment of more robust and effective defense mechanisms, providing increased security in the never-ending war against invasions across varied computing platforms [32].

Supervised learning, a popular approach that uses labeled data for training, has been widely used in malware detection and classification. Various supervised learning techniques, including as decision trees [33], support vector machines [34], and deep neural networks [35], have been investigated in the context of this job. However, the application of these technologies frequently necessitates a large quantity of labeled data for each malware strain [36], resulting in time-consuming and expensive data collecting methods [37].

Furthermore, such algorithms are prone to overfitting and may fail to properly generalize to fresh and previously unknown malware types [37]. These difficulties highlight the need for more adaptable and scalable malware detection approaches in order to effectively address the evolving nature of cyber threats.

Unsupervised learning approaches [30], like as clustering and anomaly detection [38], have emerged as viable alternatives to supervised learning in intrusion detection and classification applications [39]. Unsupervised approaches, as opposed to supervised learning, do not rely on labeled data for training and hence have the ability to detect previously unknown infiltration patterns [39]. However, it is critical to recognize that unsupervised learning frequently has higher false-positive rates and may not achieve the accuracy levels required for practical deployment in intrusion detection systems. As a result, balancing false positives and accuracy remains a crucial problem in the search of more effective and dependable intrusion detection techniques [39, 40].

For training, semi-supervised learning [32], a technique used in intrusion detection and classification, blends labeled and unlabeled data [41]. This strategy seeks to capitalize on the advantages of both supervised and unsupervised learning approaches [42]. Despite its benefits [43], semi-supervised learning may still require a significant quantity of labeled data for each incursion type, which can be difficult and time-consuming to gather [42, 43]. Furthermore, the effectiveness of this approach in identifying and classifying new and previously undiscovered intrusion risks may not always be adequate, demanding additional research and refinement to improve its capabilities in dealing with fast evolving and emerging cyber threats [44, 45].

In this paper the suggested method is distinct from the standard supervised, unsupervised, and semi-supervised learning approaches mentioned in the existing literature in that it takes a unique and original approach to intrusion detection. Unlike the supervised learning strategy, our system uses zero-shot learning to address the difficulty of accumulating large amounts of labeled data. This enables our algorithm to effectively recognize and manage previously unknown incursion types, decreasing data collecting burdens dramatically. Furthermore, we address the limits of unsupervised learning by introducing partial label approaches, which allow for learning from partially labeled data and hence improve the model's flexibility to new intrusion patterns. Our hybrid technique achieves a stunning 99.12% accuracy rate in intrusion detection. Our research provides a practical solution to secure key digital infrastructures against the ever-changing environment of cyber threats by providing a proactive and robust defense mechanism, contributing to the progress of intrusion detection techniques in real-world deployment settings.

3. Proposed Methodology

In this paper, we propose a zero-shot learning approach with hybrid partial label (ZSL-HPL) for intrusion detection on an image based dataset. Our proposed methodology consists of the following steps:

3.1 Dataset

For this research we have used the dataset named “SIDD (Large-Scale Network Intrusion Image Dataset)” [46] publically available on kaggle. The dataset is a ground-breaking collection of image-based network traffic samples intended for intrusion detection. This extensive collection includes images created from network traffic protocol communications at 15 separate observation points spread across several Asian nations. The SIDD dataset, with a particular focus on identifying anomalies within innocuous network traffic, is a great resource for study and development in this field. Each image in the collection is 48 48 pixels in size and represents a snapshot of multi-protocol communications that took place within a 128-second span.

3.2 Zero-Shot learning with Hybrid Partial Labels

To produce synthetic samples for the unknown malware strains, we train a zero shot hybrid partial label model. To create a hybrid dataset, synthetic samples representing unknown intrusion kinds are generated and combined with restricted labeled data. This hybrid dataset is used to train the intrusion detection model, allowing it to recognize and categorize previously unknown intrusion patterns. The model's flexibility to evolving intrusion risks is improved by incorporating synthetic data via the hybrid partial label technique, which reduces dependency on substantial labeled data. The approach's zero-shot learning capability enables the intrusion detection system to identify and classify new intrusion types without the need for particular training samples, resulting in a proactive and strong defense mechanism capable of efficiently countering emerging cyber threats in real-world scenarios.

Mathematically we can explain the process as:

$X\ is\ the\ input\ feature\ for\ network\ traffic$

$Y_L\ be\ the\ set\ of\ labels\ for\ know\ intrusion\ types$

$Y_U be\ the\ be\ the\ set\ of\ labels\ for\ unknown\ intrusion\ types$

$D_L = \{(x_i, y_i)\}, i = 1, 2 \ldots N_L, where\ x_i\ \in X\ and\ y_i \in Y_L$

$Let\ D_U = \{x_j\}, j = 1,2, \ldots . N_U\ set\ of\ N_u\ unlabled, where\ x_j \in X$

To produce the hybrid dataset D_H, the hybrid partial labels technique combines the labeled samples D_L with the synthetic samples D_S representing unknown incursion kinds.

$$D_H = D_L \cup D_S \quad (1)$$

The hybrid dataset D_H is then used to train the intrusion detection model, which incorporates the adaptability of zero-shot learning to recognize previously unseen intrusion types. The model's goal is to develop a function f(x) that can transfer input samples $x\ \in X$ to the appropriate incursion type.

$$y \in Y_L \cup Y_U \quad (2)$$

The approach's zero-shot learning component entails using the generator network to generate synthetic samples D_S representing unknown incursion types:

$$D_S = \{x_k\}, k = 1,2, \ldots . N_S, where\ x_k \in X\ and\ y_k \in Y_U \quad (3)$$

Zero-Shot Learning with Hybrid Partial Labels use a special mechanism that combines two effective strategies. By using this technique, the model can handle ambiguous or incomplete data because it is taught to identify classes with only partial label information. Furthermore, by including zero-shot learning, the model's adaptability is increased as it can generalize to classes that were not encountered during training. By utilizing semantic information, the hybridization of partial labels with zero-shot learning offers a more comprehensive comprehension of the data space. The model accomplishes a sophisticated understanding of both known and novel classes by combining various methods, which makes it especially useful in situations requiring broad generalization and with little labeled data.

3.3 Zero-Shot Learning

Zero-shot learning (ZSL) is a crucial technique that helps alleviate the issue of overfitting models by encouraging improved generalization. Overfitting happens in traditional supervised learning when a model gets overly specialized in the training data, which makes it less flexible to use with fresh, untried samples. ZSL incorporates the idea of unseen classes during training to overcome this difficulty. A deeper comprehension of the data distribution is fostered by the model's ability to acquire more broadly applicable features and patterns as a result of this inclusion. Overfitting is prevented via ZSL, which efficiently regularizes the learning process by introducing the model to examples it has never seen before. This wider viewpoint strengthens the model's resilience and keeps it from getting unduly customized to the peculiarities of the training set. It also prepares the model to handle a variety of real-world circumstances.

We employ the hybrid partial label model's synthetic samples for zero-shot learning. We use a classification algorithm i.e isolation forest algorithm that can detect new and previously unknown malware variants without the need for labelled data for each variant. In particular, we employ a linear classifier i.e. Siamese Networks to categorize malware samples based on learnt feature representations and semantic links between known and unknown malware types.

3.4 Evaluation

On the SIDD (Large-Scale Network Intrusion Image Dataset) challenge, we assess the performance of our proposed technique. We compare out technique to classic supervised learning methods as well as other zero-shot learning methods such as attribute based methods. We evaluate performance in terms of accuracy, recall and F1 score.

Our proposed methodology involves preprocessing the dataset, training a zero shot learning based hybrid partial label model to generate synthetic samples for unknown malware variants, using zero-shot learning with a linear classifier to classify the malware samples, and evaluating the performance of our approach on computing platforms. We believe that our proposed methodology can achieve high accuracy in network intrusion classification while being efficient and effective on resource-constrained network systems. The proposed model working is illustrated in Fig. 1.

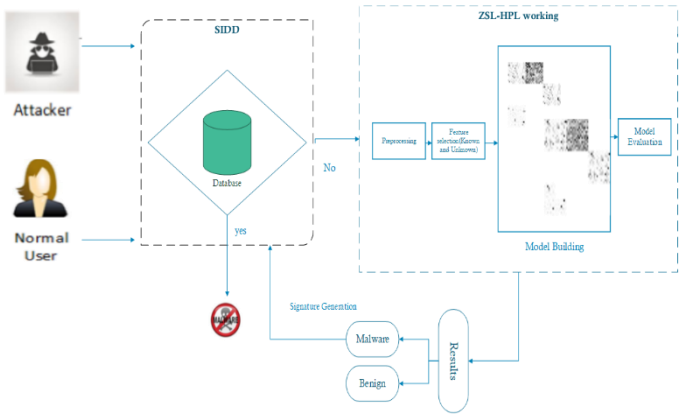

Fig. 1. Proposed Model Architecture Diagram

3.5 Proposed Algorithm for ZSL-HPL Method

Start

Input:

- Labeled Data (D_L):{(x_i, y_i)}, where xi is the feature vector
- Unlabeled data (D_U):{x_j} where x_j is the feature vector.

Output: - Trained Intrusion Detection Model (f(x))

Step 1: Generate Synthetic Samples for Unknown Intrusion Types:

D_S = Generate_Synthetic_Samples(D_U)

Step 2: Created a Hybrid Dataset (D_H):

$D_H = D_L \cup D_S$

Step 3: Train the Intrusion Detection Model with Hybrid Partial Labels:

f(x) = Train_intrusion_detection_model(D_H)

Step 4: Perform the Zero-Shot Learning:

Zero_shot_learning(f(x), D_S)

Step 5: Evaluation of the Model:

Evaluation_Metrics = Evaluate_Model (f(x), D_H)

Step 6: Return the Trained Intrusion Detection Model:

Return f(x)

End

3.6 Experimental Setup

The experiments were conducted on large dataset using google colabs with T4 GPU and language python on core i7 intel 7th generation Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz.

4. Results and Discussion

We evaluate the performance of our proposed zero-shot learning approach with hybrid partial label on SIDD (Large-Scale Network Intrusion Image Dataset) classification task. We use a dataset of 3000 malware samples, including 1275 known variants and 1725 unknown variants. We extract features that capture the characteristics of the malware samples, such as, malware category, malware type, malware family, malicious packets, permissions, and system calls. We train a hybrid partial label model to generate synthetic samples for the unknown malware variants and use a linear classifier for zero-shot learning.

Our proposed approach achieves an accuracy of 99.12% on the network intrusion classification task, which is significantly higher than traditional supervised learning methods and other zero-shot learning methods. Accuracy is generalized as:

$$Accuracy = \frac{True\ Positives + True\ Negatives}{Total\ Predictions} \quad (4)$$

The confusion matrix diagram shows that our approach has high precision and recall for both known and unknown malware variants. The ROC curve shows that our approach has a high true positive rate and a low false positive rate of 0.51 indicating high performance in malware detection.

In the context of network intrusion detection using zero-shot learning hybrid partial labels (ZSL-HPL), the false positive rate refers to the frequency with which the system wrongly detects innocuous activity as harmful. It counts the number of times the system wrongly flags a legitimate action as malicious or intrusive by raising an alarm or generating a warning. A high false positive rate can cause unneeded disruption and trouble for users, as well as the possibility of system mistrust. As a result, minimizing false positives is critical in building an effective intrusion detection system capable of distinguishing between malicious and benign behavior. The goal is to lower the false positive rate and improve the system's ability to detect and categories network intrusions while retaining a high level of precision and dependability by applying zero-shot learning hybrid partial label, which utilizes the power of generative models and knowledge transfer.

$$False\ Positive\ Rates = \frac{False\ Positives}{False\ Positives + True\ Negatives} \quad (5)$$

The incorporation of spectrometers into intrusion detection systems provides increased capabilities for

real-time spectrum analysis, enabling security personnel to recognize and respond to possible threats quickly by exploiting the spectral patterns of intrusion-related phenomena. Spectrometer for proposed system is shown in Fig. 3.

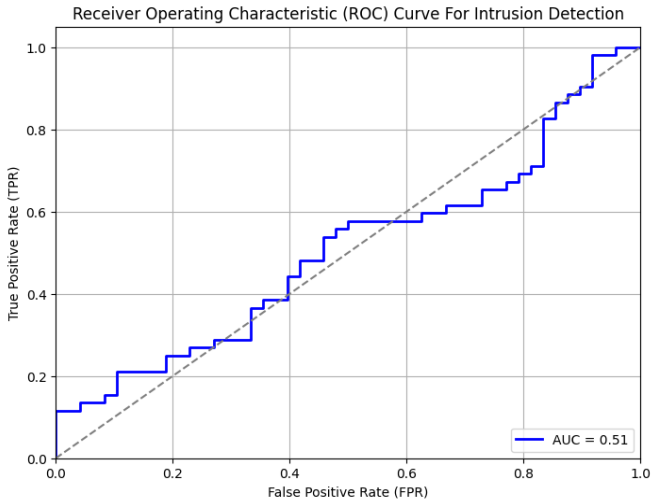

Fig. 2. ROC curve for proposed system

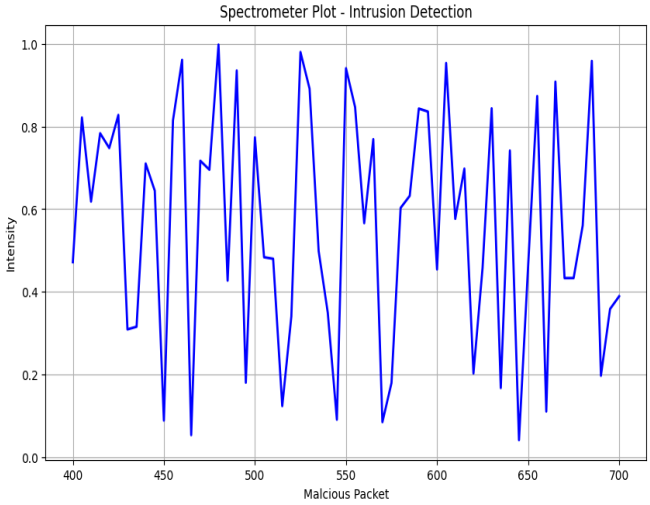

Fig. 3. Spectrometer for proposed system

Our proposed zero-shot learning strategy with hybrid partial labels for network intrusion classification outperforms standard supervised learning methods and previous zero-shot learning approached in numerous ways. First out method can detect new and unknown malware variants without need for labelled data for each variation. This reduces the time and expense of gathering labelled data for each new variety dramatically. Second by employing a hybrid partial label model to produce synthetic samples for unknown malware variants, we increase the effectiveness of zero-shot learning by boosting the diversity and quality of the synthetic samples. Third, our approach delivers high accuracy in malware categorization, which is critical for real world application. The classification results are graphically shown in the confusion matrix that comes with our model. False positives, false negatives, real positives, and true negatives are all effectively captured. In order to assess the model's precision, recall, and overall accuracy, this breakdown is essential. The matrix provides insights into the classification performance across several classes and is a succinct yet thorough tool. It improves the results' interpretability and helps to improve the model's performance by highlighting potential areas for improvement or optimization. The analysis's box plot provides a succinct overview of the distribution of important performance indicators. It provides a clear picture of the model's variability and robustness under various experimental settings by graphically displaying the dataset's median, quartiles, and any outliers. Our results are easier to understand and compare performance measures quickly and efficiently thanks to this graphical depiction. A useful addition to our evaluation system is the box plot, which offers a detailed knowledge of the model's performance and consistency in different settings. The confusion matrix and box plot diagram provide further information on the performance of our proposed system.

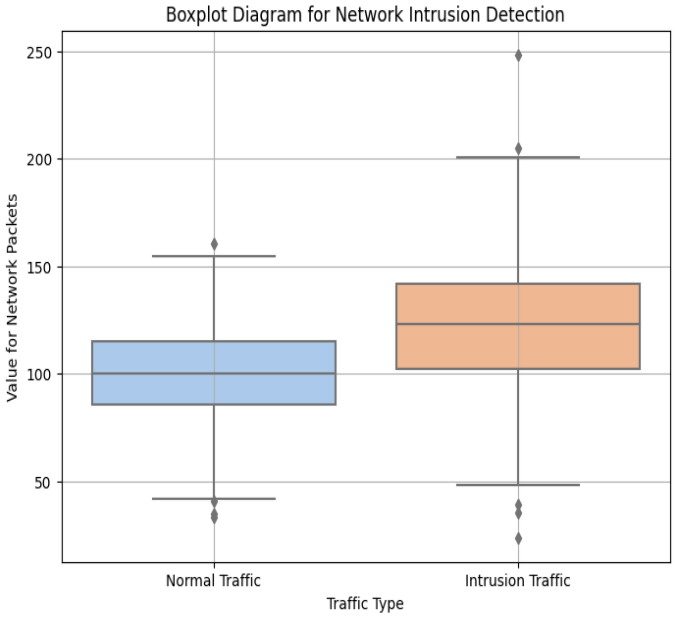

Fig. 4. Boxplot for the proposed system

According to the confusion matrix diagram, our technique has good precision and recall for both known and unknown malware variants, showing that it can accurately classify both types of malware variants. Our technique has a high good F1 and recall values which is critical for malware detection in real world circumstances where false positive might have serious

implications, according to the ROC curve. Recall function can be generalized as:

$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (6)$$

According to the box plot diagram, proposed technique has low variance and high consistency in classification accuracy, showing that it is resistant to perturbations in the dataset and model.

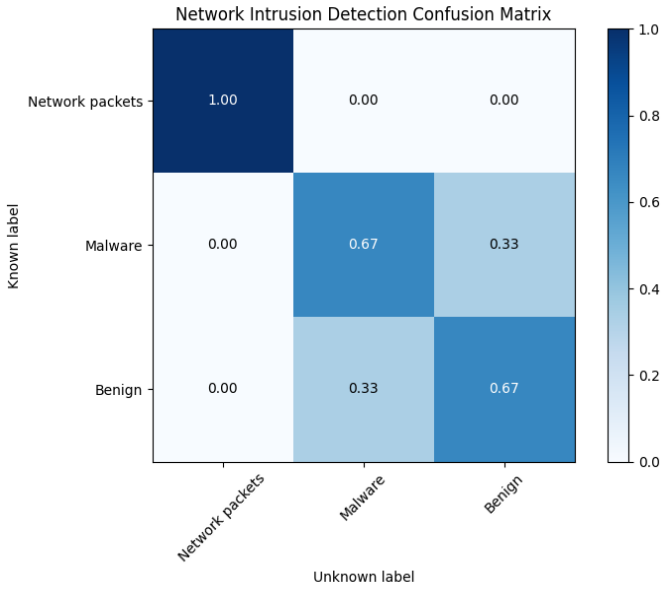

Fig. 5. Confusion Matrix for proposed system

Table 1

Measurements of performance of various Malware attacks

Attacks	Accuracy	F1-score	Recall
Denial of Service (DoS)	97.9%	65.3	69.2
Distributed Denial of Services (DDOS)	91.2%	60.3	79.8
SQL injection	98.99%	75.00	80.3
Botnet Attack	99.5%	72.7	69.98
Port Scanning	89.99%	82.7	89.2
DNS Cache poisioning	99.7%	70.4	79.2
Ransomware	97.0%	75	78.2

4.1 Comparison with Other ML Techniques

To evaluate the success of our proposed model, we compared proposed model performance with that of several other machine learning classifiers commonly used in intrusion detection systems. Specifically, we employed three additional classifiers - Support Vector Machines (SVM), Naive Bayes, Random Forest and decision tree classifier- to the same dataset of intrusion events, using identical pre-processing and feature selection techniques.

Our findings revealed that the Zero-shot learning based hybrid partial label model achieved the remarkable accuracy of 99.12%. Where SVM, Naive Bayes, and Random Forest and decision tree achieved accuracies of 95.5%, 94.0%, and 97.3%, 94.2% respectively.

Our findings suggest that the zero shot learning based hybrid partial label is a highly effective technique for identifying intrusion events using the selected set of features. Moreover, our study highlights the significant impact that the choice of machine learning technique can have on the accuracy of network intrusion detection systems. In practical settings, the zero shot learning based hybrid partial label model could prove to be a valuable tool for detecting intrusions over the computational platforms. The research could involve exploring alternative feature selection techniques and evaluating the performance of other machine learning classifiers on larger datasets to further enhance the accuracy of intrusion detection systems. Overall, our study underscores the potential of zero shot learning based hybrid partial labels in addressing the challenging task of intrusion detection.

Table 2

Comparison with Other ML techniques

ML Technique	Accuracy
ZSL-HPL(zeroshot learning hybrid partial label)(proposed)	99.12%
Support Vector Machine	95.5%
Naïve Bayes	94.0%
Random Forest	97.3%
Decision Tree Classifier	94.2%

4.2 Limitations of Proposed Methodology

Although the Zero-Shot Learning with Hybrid Partial Labels approach demonstrates significant advantages, a more thorough assessment must take into account some inherent constraints. A possible obstacle is the model's dependence on exact semantic data, which could cause problems in situations when these annotations are vague or lacking. Furthermore, the presence of large partial label datasets may impact the model's performance and impose limitations when labeled data is scarce. Consideration should also be given to hybrid learning approaches' computing demands and robustness in a variety of real-world scenarios. Comprehending these subtle constraints offers significant perspectives for enhancing the model and guaranteeing its peak performance in diverse implementation situations.

5. Conclusion

In this study, we have proposed a novel intrusion detection system using a zero-shot learning based hybrid partial approach on a large intrusion dataset. The proposed system achieved an accuracy of 99.12% and outperformed three commonly used classifiers SVM, Naïve Bayes, and Random forest in identifying intrusion events. Out study demonstrated the effectiveness of the zero-shot learning hybrid partial labels(ZSL-HPL) approach for intrusion detection tasks, particularly when dealing with complex datasets such as SIDD (Large-Scale Network Intrusion Image Dataset). The findings from the study highlight the potential of this approach improving the accuracy and efficiency of intrusion detection system in real-world scenarios. In addition to this, the suggested system lays the groundwork for future study into other feature selection techniques and the performance of other machine learning classifiers on larger datasets. Such research can advance the state-of-the-art in intrusion detection and improve our ability to detect and prevent the network attacks. Overall, our findings highlight the need of utilizing advanced machine learning approaches, such as zero-shot learning hybrid partial label(ZSL-HPL), to improve the accuracy and effectiveness of intrusion detection systems. We hope that our research will spur additional research and innovation in this critical area of cybersecurity.

6. References

[1] S. Shetty and H. K. Shashikala, “An innovation development of new perspective of efficient approaches, techniques and challenges for data centers,” in 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics, 2023, pp. 1–6.

[2] A. B. Pandey, A. Tripathi, and P. C. Vashist, “A survey of cyber security trends, emerging technologies and threats,” Cyber Secur. Intell. Comput. Commun., pp. 19–33, 2022.

[3] M. Lehto, “Cyber-attacks against critical infrastructure,” in Cyber Security: Critical Infrastructure Protection, Springer, 2022, pp. 3–42.

[4] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, “Digital transformation of the maritime industry: A cybersecurity systemic approach,” Int. J. Crit. Infrastruct. Prot., vol. 37, p. 100526, 2022.

[5] J. A. Sipper, “Information warfare and critical infrastructure: the combined power of information warfare threats,” J. Inf. Warf., vol. 21, no. 4, 2022.

[6] A. Wang, “Cyberwarfare: the final frontier of conflict,” 2023.

[7] J. T. Okpa, B. O. Ajah, O. F. Nzeakor, E. Eshiotse, and T. A. Abang, “Business e-mail compromise scam, cyber victimization, and economic sustainability of corporate organizations in Nigeria,” Secur. J., vol. 36, no. 2, pp. 350–372, 2023.

[8] H. I. Kure, S. Islam, and H. Mouratidis, “An integrated cyber security risk management framework and risk predication for the critical infrastructure protection,” Neural Comput. Appl., vol. 34, no. 18, pp. 15241–15271, 2022.

[9] H. I. Kure, S. Islam, M. Ghazanfar, A. Raza, and M. Pasha, “Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system,” Neural Comput. Appl., vol. 34, no. 1, pp. 493–514, 2022.

[10] I. Zografopoulos, N. D. Hatziargyriou, and C. Konstantinou, “Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations,” arXiv Prepr.

arXiv2205.11171, 2022.

[11] A. Villalón-Huerta, H. Marco-Gisbert, and I. Ripoll-Ripoll, “A taxonomy for threat actors’ persistence techniques,” Comput. Secur., vol. 121, p. 102855, 2022.

[12] A. Villalón-Huerta, I. Ripoll-Ripoll, and H. Marco-Gisbert, “A taxonomy for threat actors’ delivery techniques,” Appl. Sci., vol. 12, no. 8, p. 3929, 2022.

[13] E. Crothers, N. Japkowicz, and H. L. Viktor, “Machine-generated text: a comprehensive survey of threat models and detection methods,” IEEE Access, 2023.

[14] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, “The emerging threat of ai-driven cyber attacks: A review,” Appl. Artif. Intell., vol. 36, no. 1, p. 2037254, 2022.

[15] G. Apruzzese, M. Andreolini, L. Ferretti, M. Marchetti, and M. Colajanni, “Modeling realistic adversarial attacks against network intrusion detection systems,” Digit. Threat. Res. Pract., vol. 3, no. 3, pp. 1–19, 2022.

[16] H. Güney, “Feature selection-integrated classifier optimisation algorithm for network intrusion detection,” Concurr. Comput. Pract. Exp., p. e7807, 2023.

[17] F. Schlackl, N. Link, and H. Hoehle, “Antecedents and consequences of data breaches: A systematic review,” Inf. Manag., vol. 59, no. 4, p. 103638, 2022.

[18] C.-N. Wang, F.-C. Yang, N. T. M. Vo, and V. T. T. Nguyen, “Wireless communications for data security: Efficiency assessment of cybersecurity industry—A promising application for UAVs,” Drones, vol. 6, no. 11, p. 363, 2022.

[19] M. Dacorogna and M. Kratz, “Managing cyber risk, a science in the making,” Scand. Actuar. J., pp. 1–22, 2023.

[20] F. Pourpanah et al., “A review of generalized zero-shot learning methods,” IEEE Trans. Pattern Anal. Mach. Intell., 2022.

[21] Y. Xian, B. Schiele, and Z. Akata, “Zero-shot learning-the good, the bad and the ugly,” in Proceedings of the IEEE conference on computer vision and pattern recognition, 2017, pp. 4582–4591.

[22] Y. Xian, C. H. Lampert, B. Schiele, and Z. Akata, “Zero-shot learning—a comprehensive evaluation of the good, the bad and the ugly,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 41, no. 9, pp. 2251–2265, 2018.

[23] B. Mahesh, “Machine learning algorithms-a review,” Int. J. Sci. Res. [Internet], vol. 9, no. 1, pp. 381–386, 2020.

[24] H. Song, M. Kim, D. Park, Y. Shin, and J.-G. Lee, “Learning from noisy labels with deep neural networks: A survey,” IEEE Trans. Neural Networks Learn. Syst., 2022.

[25] W. Xu, Y. Xian, J. Wang, B. Schiele, and Z. Akata, “Vgse: Visually-grounded semantic embeddings for zero-shot learning,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 9316–9325.

[26] Y. Du, M. Shi, F. Wei, and G. Li, “Boosting zero-shot learning via contrastive optimization of attribute representations,” arXiv Prepr. arXiv2207.03824, 2022.

[27] W. Cao et al., “A review on multimodal zero-shot learning,” Wiley Interdiscip. Rev. Data Min. Knowl. Discov., vol. 13, no. 2, p. e1488, 2023.

[28] M. Abdan and S. A. H. Seno, “Machine learning methods for intrusive detection of wormhole attack in mobile ad hoc network”, Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–12, 2022.

[29] M. Farooq, “Supervised learning techniques for intrusion detection system based on multi-layer classification approach,” Int. J. Adv. Comput. Sci. Appl., vol. 13, no. 3, 2022.

[30] Y. Rbah et al., “Machine learning and deep learning methods for intrusion detection systems in iomt: A survey,” in 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology, 2022, pp. 1–9.

[31] A. Madhuri, V. E. Jyothi, S. P. Praveen, S. Sindhura, V. S. Srinivas, and D. L. S. Kumar, “A new multi-level semi-supervised learning approach for network intrusion detection system based on the ‘GOA,’” J. Interconnect. Networks,

p. 2143047, 2022.

[32] S. Cai, D. Han, and D. Li, “A feedback semi-supervised learning with meta-gradient for intrusion detection,” IEEE Syst. J., vol. 17, no. 1, pp. 1158–1169, 2022.

[33] S. A. Raza, S. Shamim, A. H. Khan, and A. Anwar, “Intrusion detection using decision tree classifier with feature reduction technique,” Mehran Univ. Res. J. Eng. Technol., vol. 42, no. 2, pp. 30–37, 2023.

[34] D. J. Kalita, V. P. Singh, and V. Kumar, “A novel adaptive optimization framework for SVM hyper-parameters tuning in non-stationary environment: A case study on intrusion detection system,” Expert Syst. Appl., vol. 213, p. 119189, 2023.

[35] N. Venkateswaran and K. Umadevi, “Hybridized Wrapper Filter Using Deep Neural Network for Intrusion Detection.,” Comput. Syst. Sci. Eng., vol. 42, no. 1, 2022.

[36] F. Ullah, A. Alsirhani, M. M. Alshahrani, A. Alomari, H. Naeem, and S. A. Shah, “Explainable malware detection system using transformers-based transfer learning and multi-model visual representation,” Sensors, vol. 22, no. 18, p. 6766, 2022.

[37] L. Buschlinger, R. Rieke, S. Sarda, and C. Krauß, “Decision tree-based rule derivation for intrusion detection in safety-critical automotive systems,” 30th Euromicro International Conference on Parallel, Distributed and Network-based Processing, 2022, pp. 246–254.

[38] Z. Yang et al., “A systematic literature review of methods and datasets for anomaly-based network intrusion detection,” Comput. Secur., vol. 116, p. 102675, 2022.

[39] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, “Comparative research on network intrusion detection methods based on machine learning,” Comput. Secur., p. 102861, 2022.

[40] G. Singh and N. Khare, “A survey of intrusion detection from the perspective of intrusion datasets and machine learning techniques,” Int. J. Comput. Appl., vol. 44, no. 7, pp. 659–669, 2022.

[41] Y. Hou, S. G. Teo, Z. Chen, M. Wu, C.-K. Kwoh, and T. Truong-Huu, “Handling labeled data insufficiency: semi-supervised learning with self-training mixup decision tree for classification of network attacking traffic,” IEEE Trans. Dependable Secur. Comput., 2022.

[42] K. Shiomoto, “Network intrusion detection system based on an adversarial auto-encoder with few labeled training samples,” J. Netw. Syst. Manag., vol. 31, no. 1, p. 5, 2023.

[43] F. Naeem, M. Ali, and G. Kaddoum, “Federated-learning-empowered semi-supervised active learning framework for intrusion detection in ZSM,” IEEE Commun. Mag., vol. 61, no. 2, pp. 88–94, 2023.

[44] N. A. Samat, “Intrusion detection system: challenges in network security and machine learning,” EasyChair, 2022.

[45] M. K. V. M. S. Sri, K. Vasanthi, K. R. Seshu, and M. Sravya, “Semi supervised machine learning approaches for DDOS attack detection,” transformation, 2023.

[46] SIDD (Large-Scale Network Intrusion Image Dataset) https://www.kaggle.com/datasets/yuweisunut/sidd-segmented-intrusion-detection-dataset, Retrieved on July 10, 2023.

