

Designing An Intelligent Intrusion Detection System (Ids) Using Neural Networks To Detect Zero-Day Threats

Qayssar Al-Omairi¹, Akram Hatem Saber², Haider Hadi Abbas³, Munther Hameed
Mohammed Ameen⁴, Alaa Raad Salman⁵

1. Department of Computer Engineering, College of Engineering, University of Diyala, Baquba
32001, Iraqcaser.
2. Al Hikma University College, Baghdad, Iraq.
3. Mansour University College.
4. Middle Technical University.
5. Al-Esraa University.

Abstract

The ever-growing speed of developing the network infrastructures, along with an unparalleled growth of the load of traffic flows and their complexity, has made the systems vulnerable to the advanced cyber threats. Among such, zero-day attacks present one of the most severe threats to the security requirements of a particular cybersecurity environment, being based on new vulnerabilities that may resist the signature-based defense mechanisms. The conventional intrusion detection systems (IDS) are usually unable to scale, support high-dimensional traffic, and generalize thus proving inefficient in dynamic and real-life situations.

In an attempt to overcome these issues, this research paper presents an ensemble-based intrusion detection model that will combine an autoencoder neural network and a Random Forest classifier. The suggested methodology is tested on large-scale, heterogeneous network traffic data which consists of millions of records constituting various types of attacks. results show that the ensemble model is almost optimal and has almost 99 percent accuracy, precision, recall and F1-score of known attacks. Furthermore, when training the model to zero-day attacks in which a specific set of attack types is omitted during the training process the model still has high recall (95-97%).

Key words: Zero-Day Attacks, Intrusion Detection Systems, Autoencoder, Random Forest, Anomaly Detection, Machine Learning.

1. Introduction

The modern network environment is featured with the excessive enhancements of connectivity, device diversity, and real-time traffic. On the one hand, these advances allow making operations more efficient, but, at the same time, they provide cybercriminals with more opportunities than ever before[1]. One of the most threatening risks is a zero-day attacks as these are exploitation of unidentified vulnerability with a software before a developer or a vendor can implement a software patch or mitigation measures. The unfamiliarity with such attacks makes the use of traditional IDS, which, to a great extent, is based on predetermined signatures or heuristic based on rules, ineffective[2].

Zero-day attacks are also very dangerous as they take advantage of unannounced vulnerability that has not been made public and it is extremely difficult to detect them. These exploits can be used by attackers to achieve unauthorised access, steal sensitive data, compromise network services or spread malware. More generally, the risk is increased by the magnitude and heterogeneity of network traffic with benign and malicious flows operating in complex topologies, and by the fact that the traffic features have a high-dimensionality which makes the modeling operation more complex[3].

Not only machine learning and deep learning are continuing to provide good prospects in the development of an adaptive and intelligent IDS, but it also has the potential to identify the threat that has never been observed in the past. In particular, anomaly-based detection focuses on the training of the usual behavior characteristics, and indicating an abnormality as a potential attack. Autoencoders-a form of neural network that is supposed to learn features in an unsupervised manner have been promising in this respect. Autoencoders can be trained to reconstitute normal traffic by encoding the input into low dimensional latent space and interpolating it to obtain reconstruction errors that indicates abnormal behaviour which can be used to identify novel or zero-day attacks[4].

But alone, autoencoders would fail to distinguish between benign anomalies (it is normal for traffic patterns to vary) and actual attack patterns leading to large false-positive rates. To address these shortcomings, the present work suggests implementing an ensemble hybrid IDS that would equip the autoencoders with their anomaly detection ability and allow Random Forest classifier to perform the necessary role of discrimination. The similarity between the two approaches allows a powerful mechanism on this approach, that which the deep learning is sensitive to the unknown attacks, and that which the ensemble learning is sensitive to the reduction of false positives. This framework that arises is to be capable of detecting the known and zero-day attacks in an accurate, scaleable and generalizable manner[5].

2. Problem Statement

Notwithstanding the state of advancements in the field of intrusion detection, the present-day networks are the targets of new threats and are especially susceptible to other attack types such as zero-day attacks. The attacks utilize the vulnerabilities that are unknown and make signature-based IDS ineffective. A number of issues make the development of effective detection mechanisms complicated:

- High-dimensional networks traffic: In practice, datasets of network traffic have dozens of features, such as statistics of flows, metrics at packet level, protocol flags, resulting in the scale of computational complexity and overfitting of machine learning models.
- Biases in classes: Traffic that is benign usually dominates the data, whereas attacks that are severe and infrequent are underrepresented (e.g., ransomware, DDoS). This unequal distribution is able to skew learning model and decrease the detection rates of minority attack groups.
- There are dynamic and heterogeneous environments: The behavior of a network is not well-behaved across time, devices, and protocols, and thus, it is hard to have a comprehensive comprehension of normal traffic conditions.
- Limitations on generalization: Models that are trained on a particular type of attack can be not detected by the threat they have never encountered before, which limits its practical use.
- In light of these hardships, there exists a dire requirement of an IDS capable of not only being highly precise in prevailing attack types, but also being able to generalize to zero-day attacks and achieve low false-positive rates. The proposed ensemble hybrid model will focus on curbing these problems and combining unsupervised anomaly detection with discriminative classification.

3. Research Objectives

Integrate into large, high-dimension datasets, a scalable IDS system that is able to identify known and unknown attacks in large datasets.

Use autoencoders to detect anomalies in normal network behavior so that sensitive to attacks in the network.

Add a Random Forest classifier in order to increase discriminative behavior between harmless anomalies and malicious traffic, which will come at the cost of false positives.

Test the generalization ability of the framework: simulate the zero-day conditions using the leave-one-attack-out methodology.

Make sure that it is reproducible and computationally viable by applying data preprocessing algorithms, including feature selection, and normalization.

The purpose of the study is to give a comprehensive methodology to be used in the deployment in reality network environment, that is, a reasoned-out balance between sensitivity, specificity, and scalability.

4. Zero-Day Attacks

Zero-day attack works on a vulnerability that is yet to be detected by the developers of software programs and vendors of software. The name of zero-day is under the circumstances that the developers are allocated zero days to correct the flaw before it is exploited. The personas of these strikes are particularly evil, in that [6]:

- They also happen earlier than patches get established thus they could not be detected by signature-based.
- They are erratic since both the susceptibility and the exploit are not known at the time of model training.
- They may be very harmful, such as unauthorized access, stealing of information, destructing of a service, or malware infections.
- A zero-day attack entails three important features:
- Zero-Day Vulnerability: Vulnerability is an issue in software that is not known to developers or vendors.
- Zero-Day Exploit: This is the process or code, which exploits the vulnerability.
- Zero-Day Attack: The exploit is carried out to carry out undesigned actions or damage.

Attackers usually passively provide the zero-day exploits either in the form of phishing, social engineering, malicious links, or direct exploitation. The nature of these attacks makes them unpredictable as such they require an IDS that is able to identify pattern that has never been identified. The ensemble model handles this need because it involves an autoencoder-based anomaly detection, which is sensitive to deviations and enhanced with Random Forest classification to minimize the number of false positives and improve the decision process [7].

5. Machine Learning in IDS

Machine learning allows IDS to acquire knowledge of patterns based on data, anomalies and keep up with new threats. There are two main methods that are applicable[8]:

A. Supervised Learning

There is supervised learning which is based on labeled data to train models to recognize traffic as benign or malicious. Although it has been proven effective in detecting already known attacks, zero-day attacks are not detected since the model has no examples of such a threat in the past.

B. Unsupervised Learning

Unsupervised learning, including autoencoders, identifies deviations from learned normal patterns without requiring labeled attack data. Autoencoders encode benign traffic into a latent space and reconstruct it. High reconstruction error indicates anomalies, allowing for the detection of zero-day attacks. However, benign anomalies may be misclassified, necessitating a discriminative classifier like Random Forest to reduce false positives.

6. Literature Review

The first approach to effectively detecting the presence of malware and unwanted code in the network was suggested to be the use of a random forest classifier and unified machine learning in the research of [9]. The simple feature sets were provided by two different datasets, NSL-KDD and KDDCUP99, which gave a lightweight attack detection strategy of IoT networks. The intrusion detection with a low time and energy was 99.9 percent accurate on the simulations of the proposed method using these datasets.

In testing the algorithm that is suggested in the detection of Botnet attack, KDD cup data was utilized in [10]. This algorithm was compared with the algorithms of the machine learning including Artificial Neural Network (ANN), Support Vector machine (SVM) and random Forest (RF). It was tested using performance measures like, precision, recall, F1 score and area under the curve (AUC). As per the findings, the proposed strategy had superior scores on all results with F1 0.9624.

The article in [11] introduces a new way of identifying the attack of the outlier based-zero-day cyberattacks. The overall intended purpose was to have a smart representation to detect the zero-day cyberattacks with a high percentage of detection and overcomes the limitations of the existing cyberattack detecting models. The following paper will be focused on the assessment of an autoencoder network to identify zero-day attacks. Its concept emerges due to the de-coding feature of the autoencoders. It shows elevated identification of the autoencoder model to NSL-KDD and CICIDS2017. The CICIDS2017 will detect, 90.01, 98.43, 98.47 and 99.67, GoldenEye, Hulk and port scanning as well as DDoS attacks with zero-day attacks. Besides that, NSL-KDD is the one that has a 92.96 percent accuracy. It is also contrasted to the autoencoder model versus One-Class SVM that is an outlier based machine learning technique that is not supervised. One-class SVM is the well-known unsupervised machine learning algorithm that is used to establish outliers. SVM one-class has shown the capability of detecting the zero-day attacks of the NSLKDD data and not the other attacks of the CICIDS2017 data. Auto encoder is more effective to identify data than the one-class SVM. Moreover, the amount of error (false positives) of the two models is also low.

In [12], the DoS attack intrusion to the Internet of Things was identified with the implementation of deep learning (RLSTM) intrusion detection system. The experiments on the proposed RLSTM model focused on NSL-KDD and CICIDS-2017 datasets. As a way of arriving at better performance in the classification of the outcomes, initiation to published information sets was initially filtered and subsequently utilized where the RLSTM model developed in trained it. Performance measure which was based on the accuracy, precision, recall and f-score was used to determine the effectiveness of the proposed model. The overall success of the suggested RLSTM algorithm on the CICIDS-2017 data amounted to 99.22 percent concerning the detection of DoS attacks. Moreover, it made a precision of 99.23, recall of 99.22 and f-score of 99.22 percent to detect the DoS attacks on the CICIDS-2017 dataset. This model has been found to be accurate with a high degree of 98.60 percent and is used on all the measures on performance of NSL-KDD dataset. Judging by the outcome of the

experiment, one can claim that the presented RLSTM model can be even more efficient as concerns the subject of intrusion detection. It has also proved to be most effective in the experiments, as compared to the literature proposed ones. It can thus be concluded that the proposed RLSTM can be utilized as an intrusion detection system to protect the IoT networks against the denial-of-service attacks.

The proposed concepts in the present paper [13] will make the new solid and intelligent attack detection model with the notion of heavy-hit graphs to identify the zero-day attacks. The two stages of the intended work are the signature generation and (b) evaluation. This model values its performance as compared to the signatures which have been acquired during training. The proposed zero-day attack detection has been assessed as very good in performance with an accuracy rate of 91.33 and 90.35 percent of binary attack classification and multi-class attack classification against the real time attack data respectively. The good performance of 91.62 percent is registered using the binary classification of this model using the performance in respect to the performance against the CICIDS18 bench mark dataset. In this way, the suggested solution will provide promising opportunities in terms of the identification of zero-day attacks.

In [14], the algorithm has merged hybrid deep learning, convolutional neural network, and long short-term memory (CNN-LSTM) to establish botnets attack plans, which involved BASHLite and Mirai on nine shopped IoT appliances. The scope of the conducted experimental research was expansive as it meant the use of a real N-BaIoT data that was mined out of a real system of benign and malicious patterns. The results of the test indicated that the CNN-LSTM model obtained better accuracy compared to the model with 90.88 and 88.61 detection of botnet attacks under the doorbell (Danminin and Ennio brand) model relative to the proposed system that had an excellent accuracy of 88.53 of detection of botnet attacks under thermostat brand. The precision of the advanced system to identify botnet attack using the surveillance cameras stood at 87.19, 89.23, 87.76 and 89.64 percent. In the majority of instances, CNN-LM model could identify botnet attack by different types of the IoT devices with high accuracy.

Authors in [15] came up with a suitable intrusion detection model using the concept of transfer learning, knowledge transfer, and model optimization and attempted to identify zero-day attacks successfully. The model will be configured to an application of imbalanced and regular labeled data (infrequent) of 5G IoT products. Transfer learning model represents a convolutional neural network. The structure is proved to reach the end of establishing a diverse grouping of the zero day attacks. Along this line three data set specifications sets were calculated out. According to a series of experiments, it is possible to prove that, the proposed TL-based framework can be accurate with a low false prediction rate (FPR). The suggested solution can also be linked to the increased detection of numerous families of known and zero-day attacks compared to any other previous intrusion detection system based on the DL. These findings confirm that TL is capable of determining the occurrence of cyberattack in the IoT settings.

7. Dataset and Preprocessing

The suggested framework has been tested on a massive scale network traffic data that involved millions of records and a variety of classes of attacks.

we have utilized the data, CIC-ToN-IoT-V2, that is among the most comprehensive benchmarks used to test the efficiency of the intrusion detection systems in the Internet of Things (IoT) setting. The data is made of 4,847,499 records and entails benign traffic as well

as a wide variety of cyberattacks, namely, XSS, password attacks, injection, scanning, backdoor, ransomware, MITM, DDoS and DoS. The records are separately represented by 79 features, such as features of statistical flow (e.g., flow duration, statistics of packet length, features of IAT), and features of flags (e.g., SYN, FIN, ACK counts) [16]. Table 1 shows dataset distribution.

Table 1 dataset description

Attack	
Benign	2123867
xss	2057122
password	328648
injection	269499
scanning	35564
backdoor	27145
ransomware	4790
mitm	517
ddos	202
dos	145

Figure 1 shows attack types distribution.

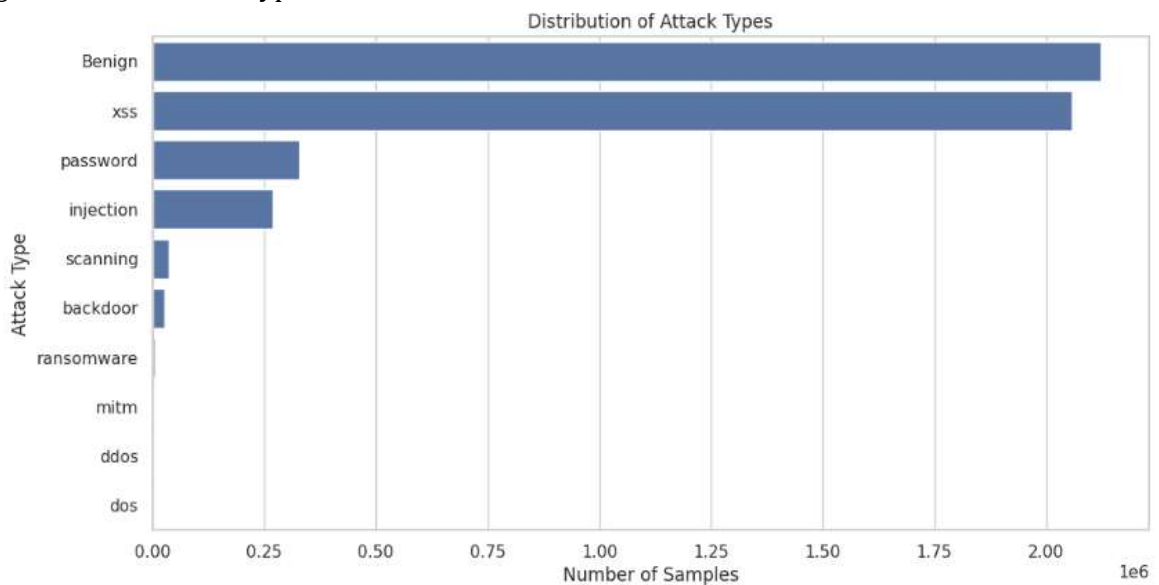


Figure 1 attack types distribution

Data Cleaning:

- Removed duplicate and incomplete records.
- Encoded categorical labels numerically.
- Standardized numerical formats (e.g., float32 for continuous values, int32 for counts).

Class Balancing:

- Used leave-one-attack-out for zero-day simulations.

Feature Selection:

- Random Forest importance ranking reduced 79 features to the top 50 most relevant.

- Dimensionality reduction improved computational efficiency and model generalization.

Normalization:

- Z-score normalization applied to all selected features to ensure balanced model training.

Dataset Split:

- 70% training, 30% testing, with zero-day test set excluding specific attack categories.

8. Methods and Protocols- Proposed Methodology: Ensemble Hybrid Model

The ensemble hybrid IDS integrates:

1. **Autoencoder:** Learns latent representations of benign traffic, identifying anomalies as deviations from normal behavior.
2. **Random Forest Classifier:** Trained on reconstruction errors and top-selected features to discriminate between benign and malicious traffic.

This combination ensures high sensitivity to novel attacks while minimizing false positives, providing a scalable and accurate intrusion detection framework.

8.1 System Workflow

1. **Data Acquisition and Cleaning:** Ensures quality and consistency of input records.
2. **Feature Selection:** Retains top 50 discriminative features via Random Forest importance scores.
3. **Normalization:** Z-score normalization standardizes feature ranges.
4. **Training Ensemble Hybrid Model:** Combines autoencoder for anomaly detection with Random Forest for classification.
5. **Evaluation:** Test set performance measured using accuracy, precision, recall, F1-score; zero-day attack simulations applied.

Figure 2 shows System Workflow.

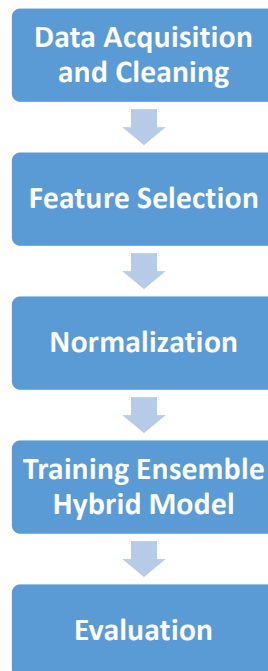


Figure 2 System Workflow

9. Performance Metrics

It can help to identify the effectiveness and accuracy of machine learning models with the help of performance metrics. They provide a notion of predictive qualities of a model and facilitate in assessing its capacity of performing different tasks. The accuracy metrics and f1score metric have been used in the study.

A. Accuracy

The accuracy is determined by the count of right predictions (out of the entire predictions) made by the model regardless of whether the prediction is positive or a negative one. To give an example, the accuracy is defined as a percentage of the correctly classified data (normal or attack data) to all the model predictions [17].

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FP} + \text{FN} + \text{TN}) \dots(1)$$

B. F1score

F- score or F 1-score is one of the measures used to evaluate a binary classification model through the predictions the model makes regarding a positive class. It is characterized in terms of accuracy and recall. It is a form of single score that is equal to recall and precision. Thus, the F1-score can be computed as the harmonic mean of the precision and the biggest quantity of the recall with the relaxation strategy of precision and recall respectively.

F-score is a mixture of the two accuracy and recall and is therefore needs to be utilized where both are vital but either of the two terms (precision, recall) is paramount to the other. As a case study, to illustrate, false negative in cases where false negative is much more than false positive, or the other way round [17].

$$\text{F-Measure} = (2 \times P \times R) / (P + R) \dots(2)$$

10. Results and Discussion

10.1 Results

To test the effectiveness of the proposed ensemble hybrid model (Autoencoder and Random Forest) a set of deep experiments was conducted. The testing has been conducted on two wider conditions, one, being, the detection of the known attacks, and the other being the generalization of the zero-day attacks through the leave-one-attack-out. The outcomes of the experiments tested the effectiveness of the standard scores of the accuracy, the precision, the recall, and the F1-score.

A. Experimental Setup

1. Training Procedure:

- The autoencoder was only trained on normal traffic with benign, which further enabled it to extract the latent features of the normal network dynamics.
- The random forest classifier was trained using reconstruction errors that were generated by the autoencoder and the top-50 highest-ranked features selected using the Random Forest feature importance ranking.
- In the training, 70% of the stratified dataset was used and the last 30 was used as raw testing.

2. Zero-Day Simulation:

- To imitate the situation of zero-day attacks, one type of attack (e.g., ransomware, XSS, or MITM) was not included in the training dataset, and it was utilized in the testing environment only.

- This was done so that the model had not been left exposed to the attack before so that its generalization abilities to new previously unknown threats could be tested.

3. Evaluation Metrics:

- **Accuracy:** This is the total percentage of the correctly classified cases.
- **Precision:** Ratio of true positive detections to all predicted positive detections, indicating false-positive reduction.
- **Recall:** Ratio of true positive detections to all actual positive instances, reflecting sensitivity to attacks.
- **F1-score:** F1-score: Precision and recall in harmonic mean which strikes a balance between sensitivity and specificity.

B. Results on Known Attacks

The ensemble model demonstrated outstanding performance on the test set containing known attack types as shown in figure 3:

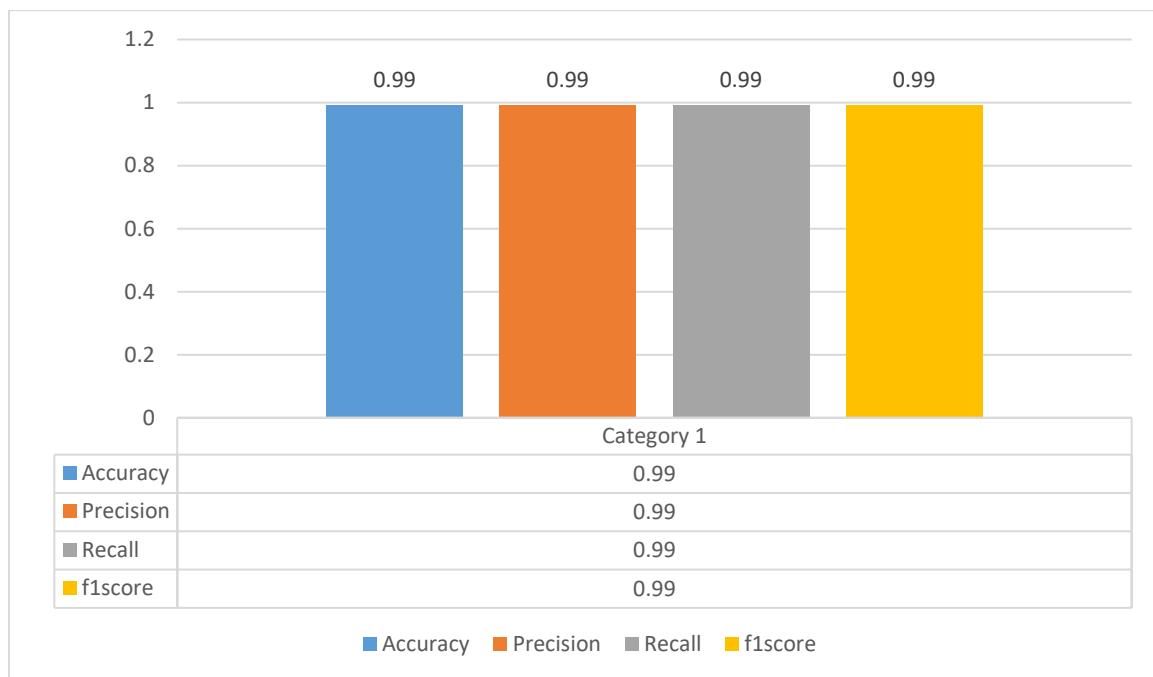


Figure 3 Results on Known Attacks

Analysis:

- The autoencoder was able to bring out a behavior which is not normal and thus the deviations are effective in anomaly detection.
- One of the useful classes to cut false positives was the Random Forest classifier, which, based on reconstruction errors, and the selected features, was quite effective in discriminating against both benign variations and attacks.
- The compounded metrics were close to perfect, which proved the collective adequacy of the combination when it comes to the usage in setting ups with intricate and high-dimensional network traffic.
- Zero-Day Attack Simulation C Results.

- The leave-one-attack-out methodology was conducted to evaluate the model fitness on detecting out of sample attacks. As an example, ransomware flows did not undergo training and were only tested.

C. Results on Zero-Day Attack Simulation

To evaluate the model's ability to detect previously unseen attacks, the leave-one-attack-out methodology was applied. For example, ransomware flows were excluded from training and used exclusively in testing. The model achieved 97 % accuracy as shown in figure 4.

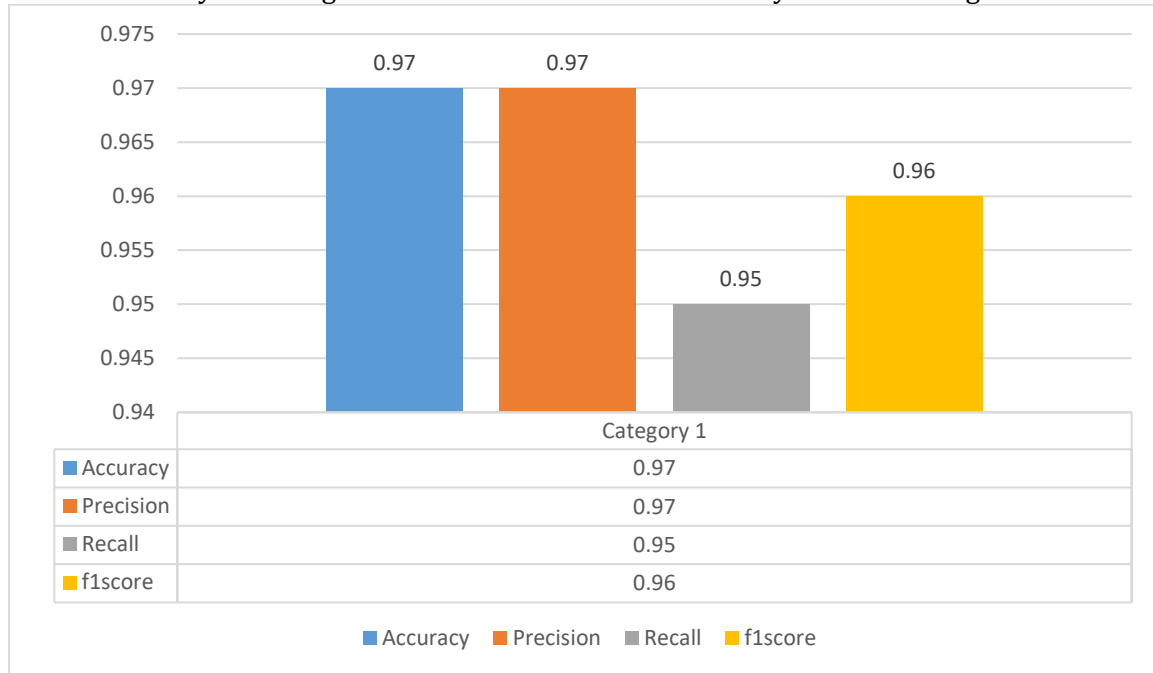


Figure 4 Results on Zero-Day Attack Simulation

Analysis:

- High recall (0.95–0.97) indicates the autoencoder's latent space effectively captured abnormal patterns corresponding to unseen attacks.
- Minor accuracy losses were also seen because the benign anomalies were occasionally misclassified, which subsequently suggests the trade-off that exists between sensitivity and specificity when dealing with zero-day cases.
- These findings reveal the model strength in extrapolating to new forms of attacks and still being practically relevant in terms of false-positive rates.

D. Key Observations

1. **Vulnerability to New Threats:** The autoencoder element is very effective to detect deviations of normal traffic, and thus, it is highly sensitive to detecting zero-day attacks..
2. **False-Positive Reduction:** The Random Forest classifier significantly reduces false alarms by learning discriminative patterns between benign anomalies and attacks.
3. **Scalability:** Dimensionality reduction via feature selection and stratified sampling ensures computational feasibility for large-scale network datasets.
4. **Realistic Deployment:** The ensemble hybrid approach has almost perfect detection rates on known attacks, and good generalization to unseen attacks, which make it

adequately applicable to operate intrusion detection of actual intrusion in real-life networks.\

All in all, the experiments affirm that the Ensemble (Autoencoder and Random Forest) model is a balanced, powerful and realistic method of intrusion detection that can easily deal with known and zero-day attacks in high dimensions network setups.

10.2 Discussion

The ensemble model combines:

- **Autoencoder:** Captures deviations in traffic for zero-day detection.
- **Random Forest:** Provides robust classification, reducing false positives.

Key observations:

1. The model is sensitive to previously unseen attacks, confirming generalization capability.
2. Dimensionality reduction and stratified sampling enable scalability.
3. The system maintains low false-positive rates while achieving near-optimal detection metrics.
4. Leave-one-attack-out methodology demonstrates robustness in realistic zero-day scenarios.

11. Conclusion and Future Work

11.1 Conclusion

This paper provides a scalable accurate and strong ensemble hybrid IDS which can be used in identifying known as well as zero day attacks. Key achievements include:

- Near-optimal performance for known attacks ($\approx 99\%$ accuracy, precision, recall, F1-score)
- High recall for zero-day attacks ($\approx 0.95-0.97$)
- Few false-positive rates and can be used in the real world.

11.2 Future directions

1. Real time implementation and monitoring.
2. As Integration with a variety of heterogeneous data.
3. Fine scale engineering and time based analysis.
4. Changing patterns of attacks modified online learning.

The proposed ensemble framework evidently presents that the unsupervised deep learning paired with ensemble classification offers an incredibly useful and effective IDS solution to current networks.

Acknowledgements

We extend our sincere thanks and appreciation to everyone who contributed to the success of this work, whether through language assistance, writing help, or proofreading.

References

- [1] Ali, Shamshair, et al. "Comparative evaluation of ai-based techniques for zero-day attacks detection." *Electronics* 11.23 (2022): 3934.
- [2] Sarhan, Mohanad, et al. "From zero-shot machine learning to zero-day attack detection." *International Journal of Information Security* 22.4 (2023): 947-959.
- [3] Guo, Yang. "A review of machine learning-based zero-day attack detection: Challenges and future directions." *Computer communications* 198 (2023): 175-185.

- [4] Zoppi, Tommaso, Andrea Ceccarelli, and Andrea Bondavalli. "Unsupervised algorithms to detect zero-day attacks: Strategy and application." *Ieee Access* 9 (2021): 90603-90615.
- [5] Zahoor, Umme, et al. "Zero-day ransomware attack detection using deep contractive autoencoder and voting based ensemble classifier." *Applied Intelligence* 52.12 (2022): 13941-13960.
- [6] Kumar, Vikash, and Ditipriya Sinha. "A robust intelligent zero-day cyber-attack detection technique." *Complex & Intelligent Systems* 7.5 (2021): 2211-2234.
- [7] Deldar, Fatemeh, and Mahdi Abadi. "Deep learning for zero-day malware detection and classification: A survey." *ACM Computing Surveys* 56.2 (2023): 1-37.
- [8] Vanin, Patrick, et al. "A study of network intrusion detection systems using artificial intelligence/machine learning." *Applied Sciences* 12.22 (2022): 11752.
- [9] Rani, Deepa, and Narottam Chand Kaushal. "Supervised machine learning based network intrusion detection system for Internet of Things." 2020 11th International conference on computing, communication and networking technologies (ICCCNT). IEEE, 2020.
- [10] Rethinavalli, S., and R. Gopinath. "Botnet attack detection in internet of things using optimization techniques." *International Journal of Electrical Engineering and Technology* 11.10 (2020): 412-420.
- [11] Hindy, Hanan, et al. "Utilising deep learning techniques for effective zero-day attack detection." *Electronics* 9.10 (2020): 1684.
- [12] Adefemi Alimi, Kuburat Oyeranti, et al. "Refined LSTM based intrusion detection for denial-of-service attack in Internet of Things." *Journal of sensor and actuator networks* 11.3 (2022): 32.
- [13] Kumar, Vikash, and Ditipriya Sinha. "A robust intelligent zero-day cyber-attack detection technique." *Complex & Intelligent Systems* 7.5 (2021): 2211-2234.
- [14] Alkahtani, Hasan, and Theyazn HH Aldhyani. "Botnet Attack Detection by Using CNN-LSTM Model for Internet of Things Applications." *Security and Communication Networks* 2021.1 (2021): 3806459.
- [15] Rodríguez, Eva, et al. "Transfer-learning-based intrusion detection framework in IoT networks." *Sensors* 22.15 (2022): 5621.
- [16] <https://www.kaggle.com/datasets/dhoogla/cictoniot>
- [17] Obi, Jude Chukwura. "A comparative study of several classification metrics and their performances on data." *World Journal of Advanced Engineering Technology and Sciences* 8.1 (2023): 308-314.