Enhancing IoT Security: A Comparative Analysis of Machine Learning and Deep Learning Techniques for Botnet Detection

Omar Almousa
Jordan University of Science and Technology, Jordan
osalmousa@just.edu.jo (corresponding author)

Batool Hamdallh
Jordan University of Science and Technology, Jordan
brhamdallh21@cit.just.edu.jo

Ruba Al-nu'man
Jordan University of Science and Technology, Jordan
rsalnuman21@cit.just.edu.jo

Received: 22 March 2025 | Revised: 3 May 2025 | Accepted: 10 May 2025

 DOI: https://doi.org/10.48084/etasr.11092

ABSTRACT

The Internet of Things (IoT) has revolutionized technological interactions but still faces significant security challenges from threats such as botnets. Therefore, effective detection methods are crucial. This study evaluates several Machine Learning (ML) and Deep Learning (DL) models for detecting IoT cyber threats, focusing on Mirai botnet attacks and ARP spoofing on the CIC IoT Dataset 2023. ML models, namely Stochastic Gradient Descent (SGD), Support Vector Machine (SVM), Decision Tree (DT), Logistic Regression (LR), and K-Nearest Neighbors (KNN), and DL techniques, namely Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN), were evaluated. The results show that data augmentation (oversampling) significantly increased performance across all models. DT and KNN achieved the highest metrics (precision, recall, F1-score, and accuracy of 0.98), demonstrating superior classification capabilities. DL models had similar results, with CNN improving from 0.96 to 0.98 after oversampling, showing its adaptability to enhanced data diversity. Conversely, SGD demonstrated high sensitivity to class imbalance, emphasizing the need for balanced datasets in IoT security applications.

Keywords-Internet of Things (IoT); Mirai; ARP spoofing; ML; DL

I. INTRODUCTION

The Internet of Things (IoT) consists of a network of devices capable of sensing, collecting, processing, and exchanging data over the Internet. As it continues to evolve, the IoT serves as a critical technology for various sectors, including medical IoT, industrial applications, and other smart environments. The projections indicate that the number of IoT devices will reach 30 billion by 2025 [1]. However, this rapid spread introduces several security challenges [2]. The dependence of various domains and applications on the IoT amplifies the potential impact of vulnerabilities [1]. Despite the growing interest in IoT security in both academia and industry, significant challenges remain that require further investigation. The Mirai botnet attack is the biggest digital threat to IoT systems and a growing concern. This malware targets IoT devices and controls them to disrupt their functionality [3]. The recent increase in Mirai attacks poses significant risks, including service outages and data breaches. To address these challenges, advanced and adaptable detection techniques are essential to counter the evolving strategies of cyber attackers.

The Mirai attack is a prominent example of a botnet attack targeting IoT devices. First discovered in 2016 [4], Mirai malware infects vulnerable IoT devices, such as routers, cameras, and other connected devices, by exploiting default login credentials. Once compromised, these devices become part of a botnet - a network of infected devices controlled by the attacker. A type of attack carried out by Mirai botnets is a Distributed Denial of Service (DDoS), where compromised devices flood the target server or network with a massive amount of traffic, making it inaccessible to legitimate users [4]. The ability of the Mirai botnet to spread rapidly and its significant impact on IoT ecosystems highlight the critical need for robust security measures to protect against such threats.

The Address Resolution Protocol (ARP) plays an important role in communication within local networks, using Internet Protocol (IP) addresses to help devices determine the hardware address of the destination [1]. ARP spoofing is an attack in which a malicious actor inserts bogus ARP information into network traffic, misleading target devices into sending their data to an incorrect destination. Through successful ARP spoofing, an attacker can intercept and manipulate network traffic, leading to unauthorized access, data compromise, and potential control of IoT devices [1]. These attacks can have serious consequences, highlighting the need for effective security measures.

This study focuses on using a Mirai and ARP spoofing dataset while employing Machine Learning (ML) and Deep Learning (DL) methods to gain insight into optimal algorithms to combat cyber threats. The objective was to leverage these sophisticated techniques to pinpoint and deploy the most effective algorithms, thereby enhancing our understanding and capacity to counter cyber threats within this specific domain. The aim was to evaluate and compare various ML and DL algorithms to determine those with optimal performance in the analysis of Mirai data. This systematic approach can help identify and deploy algorithms that offer robust and innovative solutions to address the challenges posed by cyber threats within interconnected Internet environments. Seven advanced ML and DL detection models were employed to address the challenges involved in detecting Mirai botnets and ARP spoofing in an IoT context. The ML models include Stochastic Gradient Descent (SGD), Support Vector Machine (SVM), Decision Tree (DT), Logistic Regression (LR), and K-Nearest Neighbors (KNN), and the DL models involve a Forward Neural Network (FNN) and a Convolutional Neural Network (CNN).

Researchers have been fervently exploring innovative methods to preemptively identify and thwart such attacks, aiming to fortify the resilience of IoT ecosystems against cyber threats. In [5], a mechanism was implemented to verify responses received from potential attackers, thus mitigating the risk of cache poisoning attacks. Specifically, this approach involved disregarding unregistered replies and establishing a correlation between a host's Media Access Control (MAC) and IP addresses. However, this approach may have limitations, particularly in larger network environments. Researchers commonly investigate emerging frameworks such as ML and DL algorithms and alternative anomaly detection methods, which are less limited and better suited for scalability, enabling them to outpace sophisticated cyber adversaries. The efficacy of employing ML and DL algorithms in cyber-attack detection has improved significantly. In recent years, many studies have delved into this domain, reflecting the growing importance and potential of leveraging ML techniques to enhance cybersecurity. In [6], a method was proposed to identify malicious IoT traffic using DL techniques. This approach employed a CNN to extract flow characteristics, followed by the application of autoencoders for unsupervised classification of potentially harmful IoT traffic. By employing an anomaly-based strategy, the experiments demonstrated the efficacy of this method in achieving minimal False Negative Rates (FNR) and False Positive Rates (FPR).

Botnets pose a significant threat, prompting extensive research efforts for their detection. Previous studies have shown that the application of DL techniques significantly enhances Botnet detection, yielding high accuracy and efficacy. In [7], DL methods were applied to identify botnets within an IoT ecosystem. This study employed a deep Bidirectional Long Short-Term Memory Recurrent Neural Network (BLSTM-RNN) model with word embeddings to transform textual data from captured packets into a suitable format for analysis. The findings demonstrated the efficacy of the BLSTM-RNN model in accurately detecting botnets while minimizing losses, particularly in attacks such as Mirai, UDP, and DNS floods. Despite the additional computational overhead, this model exhibited progressive improvements over time, demonstrating enhanced performance in the long term. In [8], a model was proposed to detect traffic within IoT environments, employing a diverse array of techniques to achieve optimal accuracy. Leveraging deep neural networks and ensemble learning methods, this approach achieved exceptional and swift performance in classification tasks with 99% accuracy in traffic classification, demonstrating remarkable effectiveness in identifying malicious patterns. Therefore, this model serves as a comprehensive and effective security solution for IoT environments.

In [9], a framework was designed to identify Mirai botnet attacks in IoT by employing an SVM model. SVM is adept at recognizing patterns and classifying them into separate groups, producing precise classification results even when faced with sparse training data. In [10], deep learning algorithms were employed to improve the detection of Mirai botnet attacks on IoT devices, reducing the risks associated with Distributed Denial of Service (DDoS) attacks and enhancing overall security measures. Three primary DL architectures were used: Genetic Recurrent Neural Networks (GRUs), Long Short-Term Memory (LSTM) networks, and CNNs. The findings showed that the CNN model outperformed both the LSTM and GRU models in terms of detection accuracy, precision, recall, and F1 score. In [11], the aim was to improve the precision of identifying and responding to Mirai attacks. This study employed Artificial Neural Network (ANN), SVM, and KNN, trained on variously sized datasets extracted from the Kitsune dataset. The findings showed that ANN outperformed SVM and KNN in all metrics, underscoring its effectiveness in detecting Mirai attacks.

In a recent study [3], an extensive examination of the Mirai botnet and its associated threats was performed, with a focus on mitigating the growing risks it poses. The study introduced five advanced detection models, DNN, CNN, LSTM, Random Forest- LSTM (RF-LSTM), and XGBoost-LSTM, to address the complexities of identifying Mirai botnets within the IoT framework. The results showed that ensemble models such as RF-LSTM and XGBoost-LSTM exhibited superior accuracy, exceeding 97%. These models effectively utilized LSTM to address sequence-based challenges in conjunction with the stability of the ensemble methods. The DNN model demonstrated commendable performance in terms of detection accuracy and precision, surpassing 95% and validating the effectiveness of DL in Mirai botnet detection. However, the CNN model exhibited slightly lower performance in all

metrics. The XGBoost-LSTM model showed significant true positives in all classes but encountered some challenges. In contrast, the standalone LSTM model demonstrated high true positives but also a high proportion of false positives and negatives. The integrated approach of employing LSTM alongside XGBoost with adversarial learning proved to be a successful strategy for detecting the Mirai botnet, achieving an effectiveness rate of 97.7. However, it is essential to acknowledge the limitations of the current model in addressing potential new or evolving variants of the Mirai botnet not represented in the training dataset, which may impact its efficacy.

In the realm of spoofing detection, in [12], contemporary ML methods were employed, namely LSTM and Decision Tree (DT) classifiers, to detect and predict ARP spoofing. By conducting thorough experiments across diverse datasets, this study assessed the efficacy of these models. This study highlighted the potential utility of ML approaches in effectively identifying ARP spoofing. Both LSTM and DT classifiers exhibited notable accuracy in detecting ARP spoofing instances. LSTM networks required more resources and time for training, and DT demonstrated faster performance.

In [1], an ML model called ARP-PROBE was designed to be resource-efficient and easily interpretable to address the challenge of identifying ARP spoofing incidents within IoT environments. This model demonstrated proficiency in recognizing ARP spoofing attacks by extracting crucial features from network packets, facilitated by a feature selection and extraction module. The effectiveness of this system was emphasized by its utilization of 21 meticulously chosen features extracted from IoT network packets. A notable enhancement lies in the incorporation of SHAP values, which enhance transparency and interpretability, thus fostering trust in detection outcomes. In the training phase, a DNN model was trained using a preprocessed dataset, allowing for comprehensive analysis and learning. Subsequently, in the deployment phase, live traffic packets were captured using the tcpdump tool, and features were extracted using tshark. These extracted features were then fed into the trained model for inference, evaluating each packet to classify it as either an ARP spoofing attack or benign traffic. ARP-PROBE achieved a remarkable accuracy of 99.98% alongside low FPR (0.026) and FNR (0.001).

In [13], a pioneering dynamic framework, named DL-ARP, was proposed, which merged an XGBoost classifier with a CNN-LSTM architecture. This framework aimed to promptly identify and counteract ARP spoofing attacks in real time by monitoring incoming data packets. Through the utilization of an XGBoost algorithm, relevant features crucial for classification were extracted. The incorporation of a multilayered CNN-LSTM architecture allowed the model to harness both feature generalization and memory logic flow within the layers, yielding promising outcomes across all test scenarios. The training phase culminated in an accuracy plateau of approximately 99.91, while the evaluation on test data demonstrated an accuracy of approximately 99.83, accompanied by a minimal loss of 0.0124 during the final stages. In particular, the evaluation time of the model for a new test sample of network data, sized at 2500, averaged merely 0.3926 s, translating to approximately 0.15 ms per data entry. As a result, even within expansive networks characterized by a heavy and continuous data flow, DL-ARP offers the ability to promptly detect connection anomalies without introducing delays to communicating devices.

For real-time cyberattack detection, a novel algorithm was introduced in [14], employing a randomly connected self-organizing DNN (AADRNN) developed within the IoTAC framework. This algorithm was designed to recognize attack patterns in network traffic, whether through offline or online learning during regular algorithm operation, to identify potential attacks. The AADRNN model predicted the expected values of these metrics for normal network operation and identified signal transitions indicative of attacks. Through gradual training aligned with the actual operation, the AADRNN network detects attacks using historical normal network traffic, obviating the need for attack data, thereby saving significant time and reducing learning requirements. The evaluation results demonstrated the high effectiveness of the AADRNN approach in accurately detecting various cyberattack types while maintaining low false alarm rates.

In [15], a paradigm-shifting method in cybersecurity was introduced, which integrated DL techniques for automated threat classification. Focusing on the intricate analysis of IoT device traffic patterns, this study addressed a crucial aspect of the contemporary cybersecurity infrastructure. This study used the N-BaIoT database, which includes authentic traffic data sourced from devices infiltrated by notorious botnet software such as Bashlite and Mirai. A harmonized dataset was obtained through the strategic application of resampling techniques such as SMOTE, increasing the precision and efficacy of classification processes. In addition, this study achieved compelling results, demonstrating remarkable accuracy rates in distinguishing between benign and malicious activities.

II. METHODOLOGY

A. Dataset

This study used the CIC IoT Dataset 2023 [16], which is a recent diverse and large-scale dataset. It includes 33 attacks conducted within an IoT topology consisting of 105 devices. These attacks are classified into seven types: DDoS, DoS, Recon, Web-based attacks, Brute force, Spoofing, and Mirai, as shown in Figure 1. All attacks are carried out by malicious IoT devices that target other IoT devices.

This study focused on data related to Mirai attacks and ARP spoofing. Figure 2 shows the types and frequencies of Mirai attacks and ARP spoofing in the dataset. The frequencies of the attacks are as follows: Mirai-greeth-flood occurred 5,703 times, Mirai-udpplain occurred 5,244 times, Miraigreip-flood occurred 4,509 times, and MITM-Arp- Spoofing occurred 1,835 times.

Each attack involves multiple protocols. Specifically, Mirai attacks utilize the IPV, LLC, and UDP protocols, while ARP spoofing involves the TCP and HTTPS protocols. Figure 3 shows the protocols' usage.

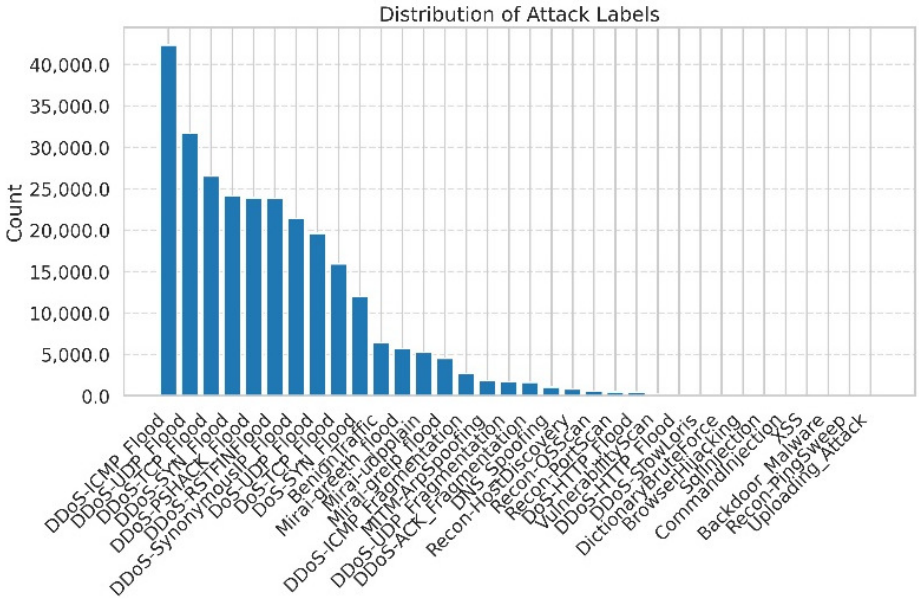

Fig. 1. Attack types and their frequencies.

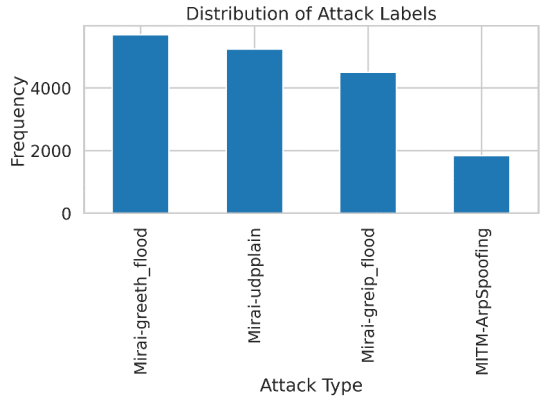

Fig. 2. Types and frequencies of Mirai attacks and ARP spoofing.

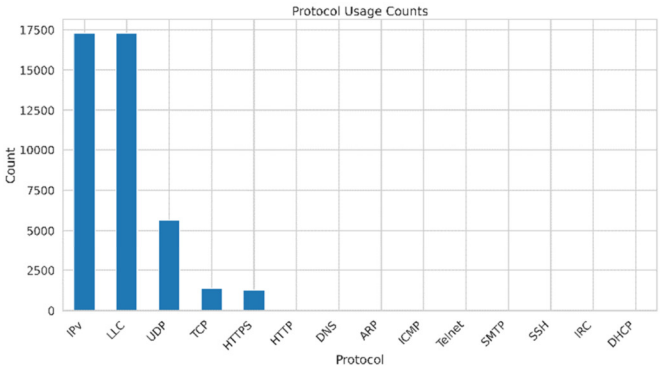

Fig. 3. Protocols' usage count.

The original dataset was unbalanced, having an unequal representation of different categories that can lead to biased model predictions. To address this problem and enhance the performance of ML models, data augmentation techniques, such as oversampling and undersampling, were applied.

Oversampling involves increasing the number of instances in the minority class(es) to balance the dataset [17]. In the context of this study, oversampling was performed on the less frequent attack types to ensure that the model learns equally from all classes. This helps to prevent the model from being biased towards the majority class [18] and improves its ability to accurately classify all types of attacks. Figure 4 shows the class distribution with oversampling.

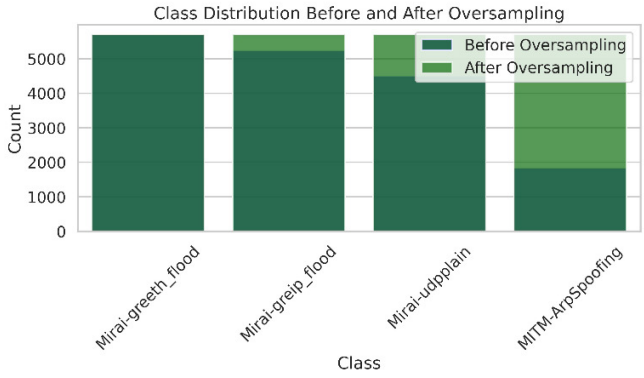

Fig. 4. Class distribution with oversampling.

Undersampling involves reducing the number of instances in the majority class to balance the dataset. This technique was applied to the more dominant classes to prevent them from overshadowing the minority classes. By undersampling, the model can focus on learning patterns from all classes equally, leading to better generalization and performance on unseen data. Figure 5 shows the distribution of the classes with undersampling.

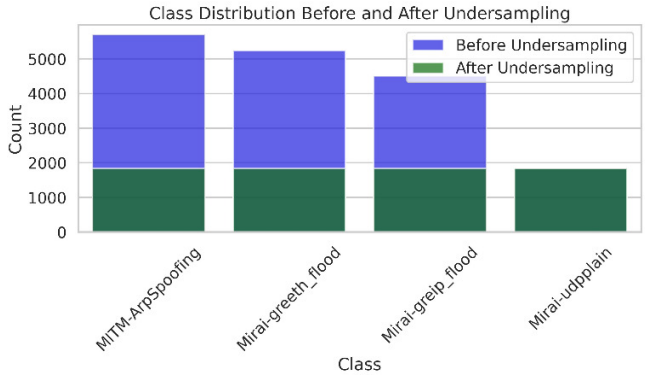

Fig. 5. Class distribution with undersampling.

B. Machine Learning Algorithms

1) Stochastic Gradient Descent (SGD)

SGD is an optimization algorithm in DL that is used to adjust the model parameters for an optimal fit between the predicted and actual outputs. Unlike traditional gradient descent, which updates the parameters using the whole dataset, SGD updates the parameters by using a single data point or a mini-batch in each iteration. This algorithm aims to reduce computation time and memory usage, making it highly efficient for large-scale and high-dimensional datasets. SGD operates with methods that use numerous training samples with minimal calculations per sample [19]. Therefore, this method is often employed as an optimization algorithm.

2) Support Vector Machine (SVM)

SVM is a classification technique commonly applied in ML tasks. Its primary function is to map data points onto a multidimensional space, with each dimension representing a specific feature. These features are assigned coordinate values, and SVM aims to create a hyperplane that effectively separates different categories or classes in the data. [20].

3) Decision Tree (DT)

A DT is like a roadmap for making choices. It is known to be fast, easy to understand, and effective even with limited data. However, when dealing with uncertain information, it can get complicated. The tree structure represents decisions visually, with questions (nodes) leading to different outcomes. It follows a divide-and-conquer approach, examining the conditions at each node until it finds the best decision [21].

4) Logistic Regression (LR)

LR is one of the methods used in supervised learning [22]. It looks like drawing a best-fit line through points on a graph to predict the chances that something will happen or not. It is great for understanding how different factors affect an outcome. This method is straightforward to grasp, making it a favorite for explaining why certain events occur. It calculates coefficients to describe relationships between factors and the likelihood of an event and then converts them into probabilities using a special function. LR helps to make sense of the data and to make informed predictions in various fields.

5) K-Nearest Neighbors(KNN)

KNN is similar to a social learner. It observes how different groups behave based on previous interactions, and then uses that knowledge to predict how new individuals will behave. The basic idea is to take K points from the available dataset, and when new points are entered, determine which category they belong to. Based on that, it determines who is closest [23].

6) Forward Neural Networks (FNNs)

FNNs are a type of artificial neural network that can learn independently from input data to complete specific tasks. In FFN, information moves in one direction, forward, from the input nodes, through hidden nodes, and finally to the output nodes. Every node in one layer is connected to every node in the next layer, making the architecture a fully connected network. Such a network is typically trained using backpropagation, which adjusts the weights of the connections to minimize the error between the predicted and actual outputs [24].

7) Convolutional Neural Networks (CNNs)

CNNs are DL models designed to process data with a network-like topology, such as images, leveraging a hierarchical structure that mimics the visual processing mechanisms of the human brain. A typical CNN architecture consists of multiple layers, including convolutional layers that apply filters to capture spatial features, pooling layers that reduce dimensionality, and fully connected layers that integrate extracted features to perform classification or regression tasks [24]. The combination of these layers allows CNNs to automatically and adaptively learn spatial hierarchies of features from input images, leading to their widespread adoption and success in various applications beyond computer vision, including natural language processing and medical diagnosis.

III. RESULTS AND DISCUSSION

The performance of various ML and DL models was evaluated using the CIC IoT Dataset 2023 [16]. The models were evaluated without any data augmentation and with two different augmentation strategies, oversampling and undersampling. Tables I-VI present the results.

A. Performance without Data Augmentation

TABLE I. PERFORMANCE OF ML MODELS WITHOUT DATASET AUGMENTATION

Classifier	Precision	Recall	F1-score	Accuracy
SGD	0.26	0.22	0.08	0.11
SVM	0.61	0.62	0.57	0.59
DT	0.90	0.90	0.90	0.90
LR	0.64	0.64	0.60	0.69
KNN	0.80	0.80	0.80	0.80

TABLE II. PERFORMANCE OF DL MODELS WITHOUT DATA AUGMENTATION

Classifier	Precision	Recall	F1-score	Accuracy
FNN	0.95	0.95	0.95	0.95
CNN	0.96	0.96	0.97	0.96

- Decision Tree (DT): The DT classifier showed the highest performance with precision, recall, F1-score, and accuracy all at 0.90. This suggests that DT is robust to the class imbalance in the dataset.
- SGD: The SGD classifier struggled significantly, with low-performance metrics across the board. This indicates that SGD is highly sensitive to class imbalance.
- SVM and LR: Both SVM and LR showed moderate performance. SVM had slightly better precision and recall compared to LR.
- KNN: The KNN classifier performed relatively well, with consistent metrics at 0.80, indicating robustness to class imbalance.
- FNN achieved exceptional precision, recall, F1-score, and accuracy, all at 0.95. This indicates its capability to generalize well and effectively learn from the dataset's features.
- CNN performed marginally better than the FNN. with precision and recall at 0.96 and F1-score and accuracy at 0.97. This highlights its strength in capturing complex patterns within the dataset.

B. Performance with Data Oversampling

TABLE III. PERFORMANCE OF ML MODELS WITH DATA AUGMENTATION (OVERSAMPLING)

Classifier	Precision	Recall	F1-Score	Accuracy
SGD	0.40	0.41	0.31	0.40
SVM	0.60	0.62	0.56	0.62
DT	0.98	0.98	0.98	0.98
LR	0.70	0.68	0.66	0.68
KNN	0.98	0.98	0.98	0.98

TABLE IV. PERFORMANCE OF DL MODELS WITH DATA AUGMENTATION (OVERSAMPLING)

Classifier	Precision	Recall	F1-Score	Accuracy
FNN	0.95	0.95	0.95	0.95
CNN	0.98	0.98	0.98	0.98

- SGD: With oversampling, SGD saw substantial improvement in performance metrics, indicating that balancing the dataset helped the classifier learn the underlying patterns more effectively.
- SVM and LR: Both SVM and LR benefited from oversampling, showing increased precision, recall, and F1 scores. This highlights the importance of addressing the class imbalance.
- DT and KNN: Both classifiers maintained high performance, suggesting their robustness and ability to leverage additional data effectively.
- FNN and CNN: Both DL techniques maintained high performance, indicating their resilience to data augmentation through oversampling.

C. Performance with Data Undersampling

TABLE V. PERFORMANCE OF ML MODELS WITH DATA AUGMENTATION (UNDERSAMPLING)

Classifier	Precision	Recall	F1-Score	Accuracy
SGD	0.24	0.34	0.30	0.44
SVM	0.59	0.56	0.48	0.57
DT	0.98	0.98	0.98	0.98
LR	0.67	0.68	0.63	0.69
KNN	0.98	0.98	0.98	0.98

TABLE VI. PERFORMANCE OF DL MODELS WITH DATA AUGMENTATION (UNDERSAMPLING)

Classifier	Precision	Recall	F1-Score	Accuracy
FNN	0.79	0.79	0.79	0.79
CNN	0.95	0.95	0.95	0.95

- SGD: Undersampling improved its performance, but not as significantly as oversampling. This suggests that while undersampling helps, oversampling provides more data diversity and hence better performance.
- SVM and LR: Both classifiers showed moderate improvements with undersampling. However, the impact was less pronounced compared to oversampling.
- DT and KNN: Both classifiers maintained high performance, indicating their robustness even with reduced data size.
- FNN and CNN: The performance of FNN dropped to 79 in precision, recall, F1-score, and accuracy, indicating its sensitivity to reduced data size through undersampling. The CNN performance had a slight decrease compared to the original and the oversampled datasets.

D. Discussion

The evaluation of various ML and DL models on the CIC IoT Dataset 2023 revealed several key findings. DT and KNN consistently demonstrated high performance across all scenarios, showcasing their resilience to class imbalance without the need for data augmentation. Data augmentation, particularly oversampling, significantly enhanced the performance of models sensitive to class imbalance, such as SGD. Oversampling provided more diverse data, leading to improved metrics in SGD, SVM, and LR. Both FNN and CNN maintained high performance across different augmentation strategies, indicating their robustness in handling both augmented and unaugmented datasets. However, the FNN showed significant sensitivity to undersampling, whereas the CNN maintained consistent performance.

For applications utilizing the CIC IoT Dataset 2023, selecting appropriate data augmentation techniques is crucial. Oversampling generally proved to be more effective in enhancing model performance, especially for models sensitive to imbalanced data distributions. This insight guides future research to optimize the effectiveness and reliability of IoT security applications. Overall, these findings underscore the importance of tailored data augmentation strategies to maximize the performance and reliability of ML and DL models in handling IoT security challenges.

IV. CONCLUSION AND FUTURE WORK

This study evaluated the performance of various ML and DL models in detecting cyber threats targeting IoT devices, specifically focusing on Mirai botnet attacks and ARP spoofing using the CIC IoT Dataset 2023. The ML models included SGD, SVM, DT, LR, and KNN, while the DL techniques evaluated were FNN and CNN. The results demonstrated the significant impact of data augmentation, particularly oversampling, in enhancing model performance across both ML and DL approaches. The best performance was consistently observed with the DT and KNN classifiers, where both achieved the highest precision, recall, F1-score, and accuracy of 0.98 with oversampling. This robust performance underscores their ability to effectively leverage the balanced dataset for accurate classification of IoT cyber threats. Additionally, the DL techniques FNN and CNN also showed promising results. Before augmentation, both FNN and CNN achieved high precision, recall, F1-score, and accuracy of 0.95-0.96. With oversampling, CNN notably improved to achieve precision, recall, F1-score, and accuracy of 0.98, demonstrating its ability to benefit significantly from increased data diversity. In contrast, SGD exhibited high sensitivity to class distribution, with substantial improvements observed when applying oversampling. This sensitivity underscores the importance of addressing class imbalance to enhance the accuracy and reliability of SGD and similar models in IoT security applications.

These findings highlight the effectiveness of both traditional ML and DL techniques in addressing cybersecurity challenges in IoT environments. They also underscore the critical role of data augmentation strategies, particularly oversampling, in improving model performance. Future research can further explore hybrid approaches combining ML and DL techniques to achieve even greater accuracy and robustness in IoT threat detection. The evaluation of ML and DL techniques on the CIC IoT Dataset 2023 suggests several avenues for future research. First, expanding the dataset to include a wider variety of IoT devices and cyber attack scenarios could help improve the models' ability to handle diverse real-world situations. This expansion would enable the development of more robust cybersecurity solutions tailored to modern IoT environments. Second, exploring new data augmentation methods, such as synthetic data generation or hybrid approaches, could further enhance model performance and scalability. Additionally, integrating anomaly detection techniques with AI models could improve early threat detection in IoT networks. Further research into explainable AI for IoT security is also essential to build trust in automated decision-making systems. These efforts aim to strengthen the reliability and effectiveness of AI in safeguarding IoT infrastructures against evolving cyber threats.

REFERENCES

[1] M. M. Alani, A. I. Awad, and E. Barka, "ARP-PROBE: An ARP spoofing detector for Internet of Things networks using explainable deep learning," *Internet of Things*, vol. 23, Oct. 2023, Art. no. 100861, https://doi.org/10.1016/j.iot.2023.100861.

[2] A. H. A. Saq, A. Zainal, B. A. S. Al-Rimy, A. Alyami, and H. A. Abosaq, "Intrusion Detection in IoT using Gaussian Fuzzy Mutual Information-based Feature Selection," *Engineering, Technology & Applied Science Research*, vol. 14, no. 6, pp. 17564–17571, Dec. 2024, https://doi.org/10.48084/etasr.8268.

[3] V. Vajrobol, B. B. Gupta, A. Gaurav, and H. M. Chuang, "Adversarial learning for Mirai botnet detection based on long short-term memory and XGBoost," *International Journal of Cognitive Computing in Engineering*, vol. 5, pp. 153–160, Jan. 2024, https://doi.org/10.1016/j.ijcce.2024.02.004.

[4] M. Antonakakis *et al.*, "Understanding the Mirai Botnet," presented at the 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1093–1110.

[5] M. Sharma and S. Ravichandra, "Design and implementation of a mechanism to identify and defend against ARP spoofing," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, Jul. 2023, pp. 1–6, https://doi.org/10.1109/ICCCNT56998.2023.10308362.

[6] R. H. Hwang, M. C. Peng, and C. W. Huang, "Detecting IoT Malicious Traffic Based on Autoencoder and Convolutional Neural Network," in *2019 IEEE Globecom Workshops (GC Wkshps)*, Waikoloa, HI, USA, Dec. 2019, pp. 1–6, https://doi.org/10.1109/GCWkshps45667.2019.9024425.

[7] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet Detection in the Internet of Things using Deep Learning Approaches," in *2018 International Joint Conference on Neural Networks (IJCNN)*, Rio de Janeiro, Brazil, Jul. 2018, pp. 1–8, https://doi.org/10.1109/IJCNN.2018.8489489.

[8] Y. O. Kolcu, A. H. Yurttakal, and B. Baydan, "Internet of Things Botnet Detection via Ensemble Deep Neural Networks," *International Journal of 3D Printing Technologies and Digital Industry*, vol. 7, no. 2, pp. 191–197, Aug. 2023, https://doi.org/10.46519/ij3dptdi.1293277.

[9] R. G. Azhari, V. Suryani, R. R. Pahlevi, and A. A. Wardana, "The Detection of Mirai Botnet Attack on the Internet of Things (IoT) Device Using Support Vector Machine (SVM) Model," in *2022 10th International Conference on Information and Communication Technology (ICoICT)*, Bandung, Indonesia, Aug. 2022, pp. 397–401, https://doi.org/10.1109/ICoICT55009.2022.9914830.

[10] A. Sharma, P. V. Mansotra, and K. Singh, "Detection of Mirai Botnet Attacks on IoT devices Using Deep Learning," *Journal of Scientific Research and Technology*, pp. 174–187, Sep. 2023, https://doi.org/10.5281/zenodo.8330561.

[11] E. Y. Güven and Z. Gürkaş-Aydin, "Mirai Botnet Attack Detection in Low-Scale Network Traffic," *Intelligent Automation & Soft Computing*, vol. 37, no. 1, pp. 419–437, 2023, https://doi.org/10.32604/iasc.2023.038043.

[12] M. Usmani, M. Anwar, K. Farooq, G. Ahmed, and S. Siddiqui, "Predicting ARP spoofing with Machine Learning," in *2022 International Conference on Emerging Trends in Smart Technologies (ICETST)*, Karachi, Pakistan, Sep. 2022, pp. 1–6, https://doi.org/10.1109/ICETST55735.2022.9922925.

[13] H. Puram, R. S. Kumar, and B. R. Chandavarkar, "Deep Learning based framework for dynamic Detection and Mitigation of ARP Spoofing attacks," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Delhi, India, Jul. 2023, pp. 1–6, https://doi.org/10.1109/ICCCNT56998.2023.10308031.

[14] E. Gelenbe and M. Nakip, "Real-Time Cyberattack Detection with Offline and Online Learning," in *2023 IEEE 29th International Symposium on Local and Metropolitan Area Networks (LANMAN)*, London, UK, Jul. 2023, pp. 1–6, https://doi.org/10.1109/LANMAN58293.2023.10189812.

[15] A. Kumari, D. Gupta, and M. Uppal, "Enhancing IoT Security in Nuclear Power Plants: Deep Learning Approaches to Detect Mirai Attacks," in *2024 5th IEEE Global Conference for Advancement in Technology (GCAT)*, Bangalore, India, Oct. 2024, pp. 1–6, https://doi.org/10.1109/GCAT62922.2024.10924052.

[16] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, Jan. 2023, Art. no. 5941, https://doi.org/10.3390/s23135941.

[17] C. Bunkhumpornpat, K. Sinapiromsaran, and C. Lursinsap, "Safe-Level-SMOTE: Safe-Level-Synthetic Minority Over-Sampling TEchnique for Handling the Class Imbalanced Problem," in *Advances in Knowledge Discovery and Data Mining*, 2009, pp. 475–482, https://doi.org/10.1007/978-3-642-01307-2_43.

[18] X. Zhou, H. Liu, C. Shi, and J. Liu, *Deep Learning on Edge Computing Devices: Design Challenges of Algorithm and Architecture*. Elsevier, 2022.

[19] Y. Tian, Y. Zhang, and H. Zhang, "Recent Advances in Stochastic Gradient Descent in Deep Learning," *Mathematics*, vol. 11, no. 3, Jan. 2023, Art. no. 682, https://doi.org/10.3390/math11030682.

[20] S. Y. Chaganti, I. Nanda, K. R. Pandi, T. G. N. R. S. N. Prudhvith, and N. Kumar, "Image Classification using SVM and CNN," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, Gunupur, India, Mar. 2020, pp. 1–5, https://doi.org/10.1109/ICCSEA49143.2020.9132851.

[21] J. R. Quinlan, "Learning decision tree classifiers," *ACM Computing Surveys*, vol. 28, no. 1, pp. 71–72, Mar. 1996, https://doi.org/10.1145/234313.234346.

[22] Z. Khandezamin, M. Naderan, and M. J. Rashti, "Intelligent detection of breast cancer with feature selection based on logistic regression and support vector machine Classification," *Journal of Soft Computing and Information Technology*, vol. 9, no. 2, pp. 115–123, 2020.

[23] Q. Kuang and L. Zhao, "A practical GPU based kNN algorithm," in *Proceedings of the 2009 International Symposium on Computer Science and Computational Technology*, 2009, pp. 151–155.

[24] L. Alzubaidi *et al.*, "Review of deep learning: concepts, CNN architectures, challenges, applications, future directions," *Journal of Big Data*, vol. 8, no. 1, Mar. 2021, Art. no. 53, https://doi.org/10.1186/s40537-021-00444-8.