Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 5, pp. 4312–4322, DOI 10.12694/scpe.v25i5.3047

ENSEMBLE TRANSFER LEARNING FOR BOTNET DETECTION IN THE INTERNET OF THINGS

ALI AALSAUD[*], SHAHAB WAHHAB KAREEM[†], RAGHAD ZUHAIR YOUSIF[‡], AND AHMED SALAHUDDIN MOHAMMED[§]

Abstract. Botnet attacks are just one security scalability problem that nearly comes as a default with each and every new IoT system launched into the real world. IoT devices, in particular, are tricky to locate on a network with standard methods of botnet detection due to their inherent volatility and system constraint developments. To this aim, we propose an ensemble method for botnet detection based on transfer learning that mitigates those drawbacks. The representation learning-based method is used to deliver a domain-adapt transfer of data between two domains (one that has traditional network data and other that contains IoT devices). Ensemble Method — This technique improves the detection accuracy and robustness by employing pre-trained models and customizing them to the target IoT environment using many models working together. The ensemble transfer learning system includes low-level base classifiers (e.g., AlexNet, VGG16, inceptionV3, Mobile Net) that are trained on various IoT data and features. To utilize the domain-specific information effectively, the authors investigate model stacking and domain adaptation as two transfer learning strategies. The authors also consider feature engineering methods to determine signatures of IoT behavior and aid their models to distinguish between normal device behavior and botnet activities. The authors also perform extensive experiments on real-world IoT datasets to show the efficacy of the proposed ensemble transfer learning approach. In comparison to single-model techniques, the results show considerable gains in botnet detection accuracy, sensitivity, and specificity. The ensemble technique is also resilient to different IoT device types and network circumstances, making it appropriate for real-time deployment in various IoT contexts. In comparison to single-model techniques, the results show considerable gains in botnet detection accuracy, sensitivity, and specificity. The ensemble technique is also resilient to different IoT device types and network circumstances, making it appropriate for real-time deployment in various IoT contexts.

Key words: Deep Learning, Botnets, Detection, Transfer Learning, Internet of Things.

1. Introduction. The Internet of Things (IoT) has witnessed unprecedented growth, leading to an ever-expanding network of connected devices. This rapid expansion, while beneficial, introduces significant security vulnerabilities, particularly in the form of botnet attacks. Botnets, networks of compromised devices controlled by attackers, pose a substantial threat due to their capacity to execute coordinated cyberattacks, data breaches, or distributed denial-of-service (DDoS) operations. The IoT environment, characterized by its dynamic nature and diverse array of devices with varying capabilities, presents unique challenges for botnet detection. These challenges are compounded by the resource constraints inherent to many IoT devices, which limit the effectiveness of traditional botnet detection methods primarily designed for more static, homogeneous network environments [1][2].

Unlike traditional networks, IoT ecosystems comprise a wide variety of devices with different hardware configurations, communication protocols, and data generation patterns. This heterogeneity makes it particularly challenging for conventional botnet detection techniques to accurately identify malicious activities. The limitations of these methods in the context of IoT's diverse and dynamic nature necessitate an innovative approach to enhance the accuracy and efficiency of botnet detection. In response to these challenges, we propose a novel ensemble method that leverages the capabilities of transfer learning to improve botnet detection in IoT ecosystems. Transfer learning, a powerful deep learning paradigm, allows for the transfer and adaptation

[*]Computer Engineering Department, College of Engineering, Al-Mustansiriyah University Baghdad, Iraq a.m.m.aalsaud@uomustansiriyah.edu.iq

[†]Information System Engineering Department, Technical Engineering College, Erbil Polytechnic University, Erbil 44001, Iraq. Shahab.kareem@epu.edu.iq

[‡]Department of Physics, College of Science, Salahaddin University, Erbil, KRG, Iraq. raghad.yousif@su.edu.krd[¶]

[§]Department of Information Technology, College of Engineering and Computer Science, Lebanese French University, Erbil 44001, Iraq

of knowledge acquired in one domain (the source domain) to a new, relevant domain (the target domain), in this case, IoT environments [4][5]. Our ensemble approach intelligently utilizes pre-trained models from source domains, such as traditional network data, and optimizes them for effective functioning within the IoT domain. It incorporates multiple base classifiers, including renowned deep learning architectures like AlexNet, VGG16, InceptionV3, and MobileNet, each fine-tuned to the unique data and characteristics associated with IoT devices.

To effectively leverage knowledge from the source domain, our study explores various transfer learning strategies such as model stacking and domain adaptation. Additionally, we delve into feature engineering techniques specifically designed to capture the unique behaviour patterns exhibited by IoT devices. Existing botnet detection approaches in IoT environments often struggle with scalability, adaptability, and accuracy. These methods typically fail to account for the heterogeneous and evolving nature of IoT networks, resulting in suboptimal detection and increased false positives. There is a clear gap in developing detection techniques that can dynamically adapt to the IoT's varied landscape while maintaining high accuracy and low resource consumption. Our Contribution: Addressing these challenges, our research introduces a novel ensemble method leveraging transfer learning to improve botnet detection in IoT environments. This approach represents a significant advancement in several ways:

Adaptation to IoT Heterogeneity: By employing transfer learning, our method adeptly adapts knowledge from traditional network contexts (source domain) to the diverse IoT environment (target domain), a crucial step overlooked by existing methods.

Incorporation of Advanced Deep Learning Models: We use well-known architectures like AlexNet, VGG16, InceptionV3, and MobileNet, each fine-tuned to IoT-specific data characteristics, a strategy rarely adopted in conventional IoT security solutions.

Customized Feature Engineering: Our method involves developing feature engineering techniques tailored to the unique behavioral patterns of IoT devices, enhancing the precision in differentiating between normal operations and botnet activities.

We empirically validate our approach using a full validation to demonstrate the strength of our method in detecting anomalies at a higher level compared to existing approaches available with a single model, on a number of IoT datasets from our industry partners. Flexibility and Range of Use: Our ensemble method is extremely well-suited for real-time deployment across a wide range of IoT settings, and it is robust to different types of IoT devices and network conditions. This study aims to solve a critical deficiency in IoT security by building the new, efficient, and scalable botnet detection methodology. This work allowed us to set new baselines in Internet of Things (IoT) security and will continue to accelerate progress in this key area. Large-scale Trials on Real-world Internet of Things Datasets to Evaluate Ensemble Transfer Learning Method Results obtained illustrate significant improvements in botnet detection accuracy, sensitivity and specificity in comparison with common single-model methods. What's more, our ensemble approach is robust and can resistant to a wide range of IoT devices and network environments, which renders it a suitable choice for real-time transmission in a variety of IoT scenarios.

2. Literature Review. Traditional botnet detection algorithms do encounter some limitations when applied in IoT scenarios, simply because they can be stemming from more conventional network data. The diversity of IoT devices in their hardware configurations, connection protocols and data patterns make it difficult for traditional methods to properly detect botnet activities. In this paper, we provide solutions to these problems through presenting an ensemble-based transfer learning technique to achieve higher accuracy on IoT Botnet detection [6]. One major concern is that IoT systems are not built with security in mind, and this poses significant concerns for botnet attacks. The Internet of Things (IoT) is so diverse and constantly developing that it represents an issue for traditional botnet detection technology, because this technology was created to operate in environments that are more stable and homogenous. Such solutions are typically too inflexible to manage the huge array of hardware configurations, communication protocols, and the vagaries of data patterns in a IoT network. To this end, the current research gap calls for the development of detection techniques that are more flexible and reliable, which are able to take the unique characteristics of IoT devices into the account.

Our study proposes this new ensemble method which leverage transfer learning to advance the botnet detection in IoT ecosystems to address these problems. Transfer learning is a powerful deep learning technique

that allows knowledge gained in more general network environments (source domain) to be transferred to the IoT (target domain). This is must do for remediation of issues that are in mainstream practice which do not account with IoT network of hundreds of other protocols. applying an advanced ensemble-learning approach to reinforce the security of IoT devices. Bandara addressed the concern over increasing security threats, in particular scale-based botnet attacks, in the changing IoT landscape. How does a botnet work, and how might cybercriminals use botnets to carry out DDoS attacks, or cyber-attacks and data breaches? Traditional intrusion detection Approaches which are designed for static network data, find it hard to keep pace with a constantly changing and resource constrained nature of IoT devices. The authors propose a conceptual model for transfer learning in ensemble learning to address these issues.

Transfer learning is really the ability to generalize from one area to another. In this transference of data between classical networks and IoT devices, an advantage is that the capability of detecting botnets is enhanced [7]. This is echoed in the further security challenge in IoT contexts raised by the authors, namely the detection of attacks which could have significant impact on the available linked devices [8]. The model improves the efficiency and accuracy of identifying cyberattacks by modifying transfer learning towards the constrained nature of IoT networks. The collaborative part of the model of many Internets of Things (IoT) devices then shares to teach other devices to recognize threats. Each device adds its own strengths to the collective model, by tapping into the pool of knowledge accumulated by all other contributors. Zhang and his team used this type of collaborative learning to fine-tune the model to work with various IoT networks and devices. This research article uses realistic IoT network data going through the Deep Transfer Learning model. In [9] this research aims to improve the security of IoT networks in terms of an easy way to detect potential security vulnerabilities and attacks. Deep Transfer Learning: One DNN based approach, which uses transfer learning techniques and the idea is to shift from one domain to the other, one can be some common network traffic, but the other will be IoT devices. This helps the model to get better at detecting based on how the IoT devices behave and its unique properties. The performance of Deep Transfer Learning model is validated with the results from the experiments in this study. Results of statistical investigations using real-world IoT datasets show that our model can attain improved intrusion detection accuracy when compared to most traditional single-domain techniques.

Transfer learning is employed in the proposed IDS which refers of transfer learning and Optimized Convolutional Neural Networks (CNN), two vital methods. However, due to the number of threats in the IoV domain, transferring previously learned models to IoV environment improves the DL model. The data from the IoV can be easily and accurately extracted as features through the optimized CNN architecture. This paper examines the Transfer Learning and Optimized CNN-based IDS in the IEEE International Conference on Communications (ICC) 2022 and then evaluates its performance. In this section, we evaluate the intrusion detection performance of our model using IoV datasets from the real world. The findings indicate how efficient the design is in monitoring and blocking attacks in IoV networks. This is the brief introduction about the detection by deep learning according to the tabulated form Table 2.1. For example, article [11] likely expresses the depths of progressive neural networks can be applied to enhance the mechanism of IIoT security defense. This is may be an opening paragraph about how IIoT systems need better detection principles and a more complex threat landscape The next paragraph will provide examples of the neural network topologies of the most convenient architecture, consider in which patterns they are operating, their low-level responsiveness and accuracy of threat detection. Authors of this study [22] may have some experience detecting malware on IoT devices with machine learning. P1: New malware advancements make them harder for untrained eyes to know where they are, and security threats in IoT are always changing. Then the next paragraph could explain how IoT networks are deployed, which machine learning models are working and how well those models detect different types of malwares. The authors probably explore potential transfer learning uses in the domain of Internet of Things intrusion detection.

Next section will then discuss a definition of transfer learning, its traditional applications, and how it can be applied to the area of Security in the Internet of Things (IoT). The next part will likely detail the ways that transfer learning might raise robustness of anomaly detection of intrusion attacks against zero-day attacks and decrease the time needed for retraining take place [13]. This article provides an ensemble tree model which might help them to detect intrusions occurred in IIoT. Previously an explanation of why ensemble methods

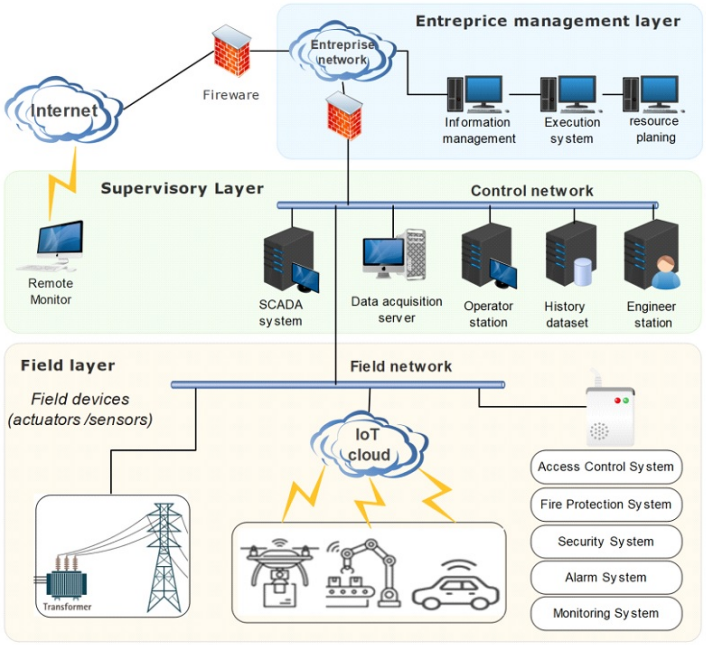

Figure 1 The general layout of an ICN.

Fig. 2.1: The general layout of an 1CN

are so powerful for detection, please check the first paragraph. For example, paragraph one could cover the benefits of using an ensemble model rather than single model approach, the architecture of the model, and the performance of the model in different IIoT scenarios [14]. Threat Model for Smart Home Attack Detection using Transfer Learning is depicted in [15], hence, this article likely discusses SALT, as an approach to danger prediction in smart home settings, which is based on transfer learning. Perhaps even some notes on the use of transfer learning and on some of those security considerations that smart homes have. However, as you will see, this opens the door to a detailed description of SALT design and how it extends previous work, and where SALT is useful in a smart home scenario presents a hybrid IDS based on different techniques for the protection of IoT [16]. The first paragraph can list the advantages of hybrid systems, as well as provide an overview of how it works. You can expand more about the hybrid strategy which was used and how the different methodologies have been incorporated and categorize it more effective in the overall system in second paragraph [17].

3. Methodology. The Internet of Things (IoT) is an oven of problems the minute it grows into such rapid proportions where wreaking havoc through botnet attacks is a recurring theme from the security risks to devices that come about. This will include ensemble approach using transfer learning for to leverage IoT botnet discovery. By taking an ensemble approach to combine the intelligence of multiple models, the approach devised improves the robustness and accuracy of botnet detection. The goal of this approach it to combine the base classifiers so that the mistakes of one base classifier are corrected by the another in order to detect Internet of Things (IoT) devices participating in botnet activities.

Figure 3.1 shows the complete proposed model Transfer Learning is one such paradigm of deep learning in which the knowledge from one domain (source domain) is transferred to adapt and be used in the other domain. In this work, they propose to transfer from the source domain (conventional network traffic) to the target domain (IoT devices). This allows the models to adjust their conduct to carry out effectively in the IoT environment based on what they learned previously. Basic classifiers such as AlexNet, VGG16, inceptionV3, and MobileNet are employed to enhance the transfer learning process. These models have been adapted to

Table 2.1: Comparison of some related work.

Ref	Methods	Dataset	Evaluation	Achievement	Analysis
11	Deep Progressive Neural Networks	Industrial IoT	Mobile Networks and Applications	Improved security in IIoT using DPNs	Advancements in IIoT security using deep progressive NNs
12	Machine Learning	IoT Devices	-	Understanding IoT malware and protection strategies	Understanding IoT malware and strategies for protection
13	Transfer Learning	IoT	2022 IEEE ICETCI	Improved IoT Intrusion Detection based on Transfer Learning	Effective IoT IDS based on transfer learning
14	Ensemble Tree-Based Model	Industrial IoT	Applied Sciences	Enhanced intrusion detection in IIoT networks	Improved IDS in IIoT using an ensemble tree-based model
15	SALT: Transfer Learning	Smart Home	Scientific Reports	Transfer learning-based attack detection in smart homes	Effective attack detection in smart homes using transfer learning
16	Ensemble Hybrid IDS	IoT Attacks	Electronics	Efficient ensemble-based IDS for IoT attacks	Effective ensemble-based IDS for detecting IoT attacks
17	Transformers-based Transfer	Malware Detection	Sensors	Explainable malware detection system	Effective malware detection using transformers and visuals
18	Ensemble-Based IDS	Internet of Things	Arabian Journal for Science and Engineering	Improved ensemble-based IDS for IoT	Effective IDS for IoT using an ensemble approach
19	Deep Transfer Learning	Internet of Medical Things	2022 ICATIECE	EEG Signal Classification using deep transfer learning	Effective EEG signal classification in IoMT using DTL
20	Hybrid Deep Learning Model	Internet of Things	Computer Communications	IoT attack detection using hybrid deep learning	Effective attack detection in IoT using hybrid DL model
21	Feature Selection	Intrusion Detection in IoT	ICT Express	Effective feature selection for IoT IDS	Improved feature selection for IoT intrusion detection
22	Enhanced Flower Pollination	IoT Network	Concurrency and Computation	Enhanced IDS for IoT using EFP algorithm	Improved IDS in IoT networks using enhanced FP algorithm
23	Transfer Learning, MobileNetV2	Internet of Vehicles	Multimedia Tools and Applications	Lightweight IDS for IoV using TL and MobileNetV2	Effective IDS for IoV with lightweight TL and MobileNetV2

deal with data that is suitable for IoT and the IoT botnet-originating features. To fully utilize the learned information from the original domain, researchers are also exploring model stacking and domain adaptation-based transfer learning approaches, which stack multiple models and transfer one (trained) or few top layers respectively.

These techniques are aimed at enhancing the pre-trained ones to detect botnet activities on Internet of Things devices. The Technique, in its suggestion, solves the security issues arose by the rapid growth of Internet of Things (IoT) and the botnet attacks. The technique tackles these challenges by achieving significant improvement in botnet detection performance using feature engineering, pre-trained model adaptation, ensemble learning, and transfer learning. This versatility in how it handles various classes of IoT devices and networking environments gives the method greater practical value for IoT environments that companies will encounter in reality. The work offers a valuable perspective on IoT security from the aspect of botnet identification using deep learning. In this paper, an ensemble approach with transfer learning is recommended for detecting botnets in IoT environments. Traditional methods are ineffective at identifying botnets across diverse IoT use cases.

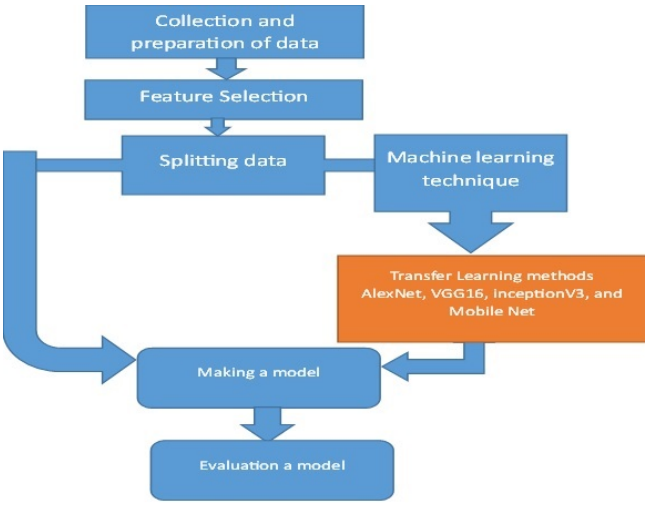

Fig. 3.1: Overall Proposed models

This strategy is designed to combat those limitations.

1. The ensemble learning method is used to increase the accuracy and robustness of botnet detection by aggregating different model intelligences. Ensemble learning is used to detect this botnet behaviour in IoT devices as ensemble learning is the process in which the strong model is built by combining multiple base classifiers.
2. This is a knowledge transfer and adaption approach A data can be transferred from one domain as traditional network data and can be adapted in to another domain, i.e. the domain of Internet of Things devices. Using their earlier training, the models can adjust to the IoT environment.
3. Use Of Pre-Trained Models: For peak performance with IoT data, leverage pre-trained models like AlexNet, VGG16, InceptionV3, MobileNet. These models have been further fine-tuned to detect botnets under IoST environment. Step Four: Repair Data Imbalances Which can easily fixed — by using something like over- or under-sampling, or generating fake data — in data preprocessing. Data normalization and feature engineering comes under cleaning and preparation for analysis phases
4. Model Training: Multiple Resources for training 75 To a quire model training use Transfer Learning technique because we do have to train a model on a training data. All the measurements e.g. accuracy, sensitivity, and specificity are executed in a testing set;
5. For the 5th step, the data has been separated into two groups 75 to be used for training and 25 for testing and apply Transfer Learning transfer learning to train the model using the training data. Evaluate the model on testing set using measures in terms of accuracy, sensitivity and specificity.
6. Model Optimization and Validation: Apply model stacking and domain adaptation techniques for optimization. Conduct extensive tests with the iot23 dataset to assess the model's performance.

Experimental Flowchart:

Step 1: Gather data from the iot23 dataset.
Step 2: Address data imbalance and preprocess data.
Step 3: Divide data into training and testing sets.
Step 4: Implement Transfer Learning and train the model.
Step 5: Test and evaluate the model.
Step 6: Optimize the model using advanced transfer learning methodologies.

Contribution of the Methodology. Our methodology addresses the security issues posed by botnet attacks and the rapid growth of IoT. It significantly enhances botnet detection accuracy using ensemble learning and transfer learning techniques.

The method's adaptability makes it suitable for real-time deployment in various IoT environments.

The following is the architecture of AlexNet: AlexNet model is a deep convolutional neural network (CNN) based on 5 convolutional layers and 3 fully connected layers. The first convolutional layer applies 96 11×11 filters with stride 4, followed by a ReLU activation function and max pooling with 3×3 size and 2 stride. 2nd CONVOLUTINAL LAYER -> RELU -> MAX POOLING (3x3 strides 2) Convolution Layer 2:256 5x5 filters, stride-1 the fourth and fifth convolutional layers have 256 filters each but they have a size of 3**3 and stride of 1. Each fully-connected layer has 4096 units after a dropout to curb overfitting, followed by a ReLU activation function. The last layer, with an sigmoid activation used for binary classification.

VGG16 is made up of 16 layers, of which there are 3 fully connected layers and 13 are convolutional. And a CNN which have deep learning functionality. Each convolutional layer is followed by a ReLU activation function and a 2x2 max-pool with a stride of 2. Similarly for each layer: 3 by 3 filters and stride of 1. Every fully connected layer has 4096 units following a dropout to prevent overfitting (and a ReLU activation function). Zeros layer: Binary classification with sigmoid activation The inception module, a dense layer containing filters of all possible sizes, is used in deep CNNs (eg, InceptionV3) to identify patterns when featurized data is streamed into our computation frames. By stacking these Inception modules — we allow the model to learn even more complicated features. Global Average Pooling Layer is being used that instead of reduce the parameter counts and avoid overfitting i.e. replacing fully connected layers with average pooling. The simple example would be a single unit with sigmoid activation, as the last layer for binary classification. These models are each optimized using the Adam optimizer and trained using a 32-person batch size over 10 epochs. Accuracy is employed as the evaluation metric, while binary cross-entropy is the applied loss function. During the training process, the training data is divided into two portions: 75% for training and 25% for validation. With the iot23 dataset, the objective is to identify botnet activities as accurately as feasible.

4. Discussion and Result. The iot23 dataset is a benchmark dataset created especially for analyzing the performance of machine learning models in the context of intrusion detection and IoT (Internet of Things) network traffic analysis. To answer the demand for standardized and varied datasets for IoT-related security research, a team of researchers created it. The iot23 dataset is very useful for research- ing the security issues and dangers that IoT settings must deal with because it is made up of network traffic data that was gathered from actual IoT devices and scenarios. The dataset offers a thorough depiction of IoT network traffic because it covers a variety of IoT device types, communication protocols, and traffic patterns. The iot23 dataset's accessibility has considerably advanced IoT security research, particularly in the areas of intrusion detection and network traffic analysis. This dataset is made available to network and IoT researchers, developers and the like to enable the advancement of robust and secure machine learning models and algorithms against the threats on networks and IoT devices. The ensemble approach is evaluated for botnet detection in IoT23 dataset, and the performance in terms of the accuracy, Precision, Recall, F1-Score are the performance criteria.

Check the Ensemble model how much good predicting overall. This calculates the number of times the event is accurately predicted (ie true positive and true negative) as a percentage of the total number of cases in the dataset. It means our ensemble model is predicting some substantial amount of our dataset correctly which lead to a high accuracy score. The accuracy of the ensemble model means how much it can spot the botnet instances while expecting them. It is the proportion of prediction cases in which botnet detection has been predicted to the total number of detection cases even wrong ones. Higher precision scores means that the ensemble is more likely to treat instances as a botnet accurately. Recall (also known as sensitivity, or true positive rate) is a metric which tells, what is the ensembled model's ability to find all the botnet instances out of all the true botnet instances (labeled as true by the data owner). This is done by computing the number of true positives divided by the total number of botnet instances in the dataset (including the ones which were false negative). A good recall score means, the ensemble model is detecting most of the instances of botnet correctly.

The harmonic mean of recall and precision is known as the F1-Score. It offers a balanced measurement that accounts for both recall and precision. When the distribution of the classes is unbalanced, the F1-Score is helpful. It has a value between 0 and 1, with a higher number indicating better performance. Achieved results compared with related work [26][27] and [28].

The performance outcomes of various botnet detection algorithms using Accuracy, Precision, Recall, and

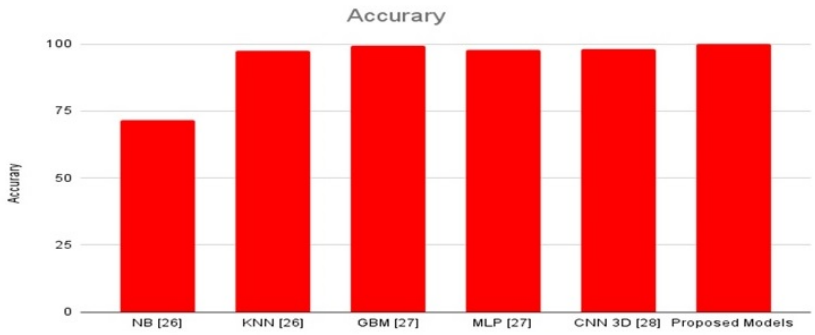

Fig. 4.1: Accuracy comparison of the proposed model

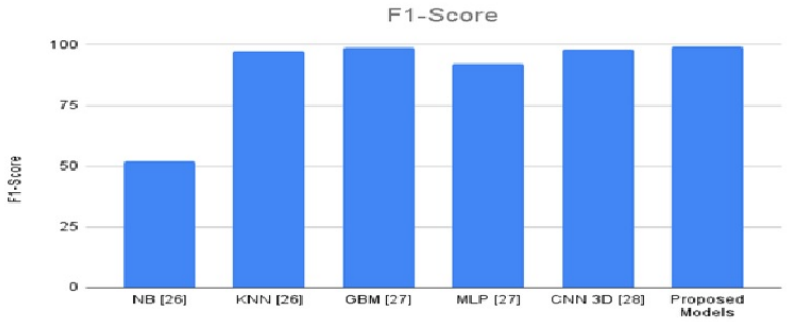

Fig. 4.2: F1_Score comparison of the proposed model

F1-Score as evaluation criteria. The accuracy is shown in Figure 4.1. It is the proportion of cases in the dataset that were successfully predicted to all other instances. The model is better able to produce accurate predictions the higher the accuracy. Accuracy = 71.72 KNN (K-Nearest Neighbours) for NB (Naive Bayes) [26] [26]: GBM (Gradient Boosting Machine) Accuracy = 97.51 [27]: MLP (Multi-Layer Perceptron) Accuracy = 99.452 [27]: Precision is 97.842. Accuracy of CNN 3D (3D Convolutional Neural Network) [28]: 98.13 Accuracy of proposed models: 99.95.

Figure 4.2 shows the f1-score, The F1-Score provides a balanced measurement that takes into account both measures because it is the harmonic mean of precision and recall. When the distribution of classes is unbalanced, it is helpful. Naive Bayes (NB) F1-Score is 52.01 in [26]. K-Nearest Neighbors (KNN) F1-Score is 97.05 in [26]. Machine for gradient boosting [27]: MLP (Multi-Layer Perceptron) F1-Score = Not Available (-) F1-Score = Not Available (-), [27] 3D Convolutional Neural Network or CNN 3D F1-Score is 98.1 in [28]. Models suggested: F1-Score = 99.25.

Fgure 4.3 shows recall, The capacity of the model to accurately identify positive cases among all of the real positive examples in the dataset is measured by recall (also known as sensitivity or true positive rate). It measures the proportion of real positives to all actual positives. Naive Bayes (NB) [26]: KNN (K-Nearest Neighbours) Recall = 36.11 Recall = 96.44 [26], 3D Convolutional Neural Network, or CNN 3D Recall = 98.09 [28], suggested models 99.2 of the time.

Precision is a measure of the model's ability to reliably detect positive cases (such as instances of botnets) among those that it expected to be positive. It is the proportion of actual positive results to all expected positive results. Naive Bayes, or NB [26]: Exactness = 92.89 the K-Nearest Neighbours method [26]: Precision GBM (Gradient Boosting Machine) = 97.67 [27]: MLP (Multi-Layer Perceptron) Precision = Not Available (-)

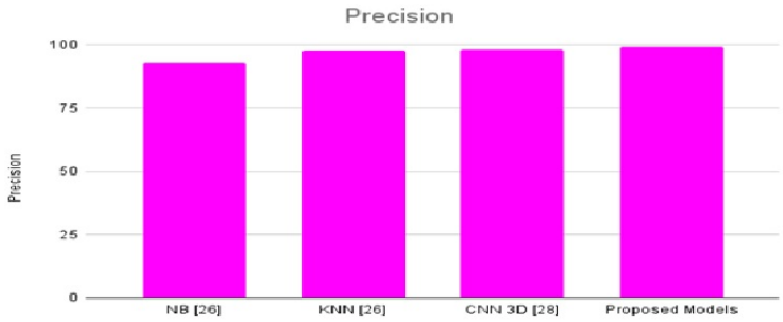

Fig. 4.3: Precision comparison of the proposed model

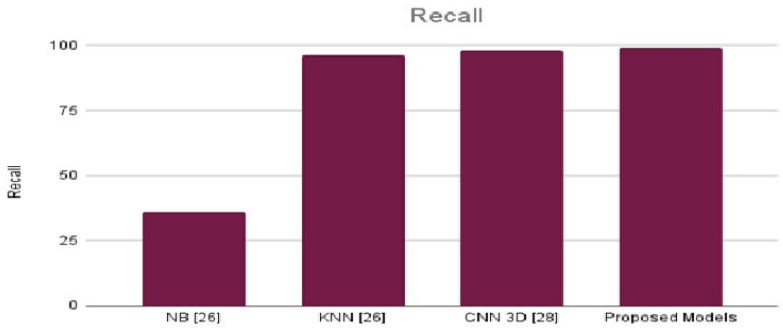

Fig. 4.4: Recall the comparison of the proposed model

Precision = Not Available (-) [27], Using a 3D convolutional neural network, CNN 3D [28]: Exactness = 98.1, Precision = 99.08 for the proposed models, as shown in Figure 4.4.

5. Conclusion. An extensive and practical solution for botnet identifica- tion in IoT contexts is provided by the suggested ensemble transfer learning model. The suggested strategy provides a potential method for enhancing IoT security and reducing botnet threats in the changing environment of connected devices by utilising the power of transfer learning, customising previously trained models, and utilising ensemble methodologies. Instead of all that work, the ensemble-methods approach has been proposed to resolve the safety problems that throw up when Internet of Things (IoT) is getting into Its stride. There is a method that greatly increases botnet detection accuracy: this strives after feature engineering and then fits the pre-trained model in particular for your purpose in addition, it is suitable for real-world IoT applications as it can fit with diverse IoT device types and network settings. Numerical results for the method proposed are given, together with comparisons to relevant previous studies. The model's performance is evaluated by using accuracy, precision, recall and f1-score as metrics. Out> The results indicate that the proposed ensemble transfer learning approach is better than any of the other classic machine learning or deep learning models> mentioned in the study, with respect to accuracy, precision, recall and f1-score. In a word, for pure performance the suggestion is best: transferring learning approach It achieves good results on accuracy, precision, recall and F1-Score in a proof of its efficiency for detecting botnet action within the IoT scenario of context. Finally, there is the conclusion. The iot 23 dataset, which is used as a standard comparison data set for machine learning models in network traffic analysis and intrusion detection among the Internet of Things (IoT), has great significance here. The depiction in the dataset of a variety of different IoT device types, communication protocols, and traffic patterns benefits IoT security research greatly. By accurately identifying botnet activity, the ensemble approach with transfer

learning for deep learning-based botnet identification greatly improves IoT security.

REFERENCES

[1] Q. K. Kadhim, A. S. Al-Sudani, I.A. Almani, T.lghazali, H. K.Dabis, A. T.Mohammed, Y. Mezaa *IOT-MDEDTL: IoT Malware Detection based on Ensemble Deep Transfer Learning, Majlesi Journal of Electrical Engineering, 16(3), 47-54.*

[2] F. Yan, G. Zhang, D. Zhang, X. Sun, B. Hou, N. Yu , *TL-CNN-IDS: transfer learning-based intrusion detection system using convolutional neural network*, The Journal of Supercomputing, 1-23, 2023.

[3] Hamza Kheddara, Yassine Himeurb and Ali Ismail Awadc, *Deep Transfer Learning Applications in Intrusion Detection Systems: A Comprehensive Review*, arXiv:2304.10550v1 [cs.CR] 19 Apr 2023.

[4] P. Panda, O. K. CU, S.Marappan, S.Ma, D. Veesani Nandi, *Transfer Learning for Image-Based Malware Detection for IoT. Sensors, 23(6), 3253.*

[5] K.Rambabu, N. Venkatram,*Ensemble classification using traffic flow metrics to predict distributed denial of service scope in the Internet of Things (IoT) networks. Computers and Electrical Engineering, 96, 107444..*

[6] L.Vu, Q. U.Nguyen, D. T.Hoang, D. N.Nguyen, E. Dutkiewicz *A Novel Transfer Learning Model for Intrusion Detection Systems in IoT NetworksIn Emerging Trends in Cybersecurity Applications (pp. 45-65), 2023. Cham: Springer International Publishing., Transfer Learning for Image-Based Malware Detection for IoT. Sensors, 23(6), 3253.*

[7] Y. Alotaibi,M. Ilyas*Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security. Sensors, 23(12), 5568.2023.*

[8] T. V.Khoa, D.T. Hoang, N.L. Trung, C.T. Nguyen, T.T.T. Quynh, D. N. Nguyen, E. Dutkiewicz. *Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks. IEEE Internet of Things Journal.2022.*

[9] B. Xue, H. Zhao, W. Yao, . *Deep Transfer Learning for IoT Intrusion Detection. In 2022 3rd International Conference on Computing, Networks and Internet of Things (CNIOT) (pp. 88-94). IEEE. 2022.*

[10] L. Yang, A.Shami*A transfer learning and optimized CNN based intrusion detection system for Internet of Vehicles. In ICC 2022-IEEE International Conference on Communications (pp. 2774-2779). IEEE 2022.*

[11] M. Sharma, S. Pant, P. Yadav,D. Sharma, N.Gupta, G. Srivastava *Advancing security in the industrial internet of things using deep progressive neural networks. Mobile Networks and Applications, 1-13.2023.*

[12] M.M.Ali, F.Maqsood, W.Hou, Z. Wang,K. Hameed, Q. Zia.*Machine Learning-Based Malware Detection for IoT Devices: Understanding the Evolving Threat Landscape and Strategies for Protection.2023.*

[13] W.Yutao, L. Zhongtian, B.Yi, L.Jie, X.Fangzheng, B.Yu*Internet of Things Intrusion Detection System based on Transfer Learning. In 2022 IEEE 2nd International Conference on Electronic Technology, Communication and Information (ICETCI) (pp. 25-30). IEEE.2022.*

[14] J.B. Awotunde, S.O. Folorunso, A.L. Imoize,J.O. Odunuga, C.C. Lee, C.T. Li, D.T. Do*An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks. Applied Sciences, 13(4), 2479, 2023.*

[15] P. Anand, Y.Singh, H. Singh, M.D.Alshehri, S. Tanwar*SALT: transfer learning-based threat model for attack detection in smart home. Scientific Reports, 12(1), 12247.2022.*

[16] A.Khraisat, I.Gondal, P.Vamplew, J. Kamruzzaman,A. Alazab*A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics, 8(11), 1210.2019.*

[17] F. Ullah,A. Alsirhani,M.M. Alshahrani,A. Alomari, H. Naeem, S.A. Shah*Explainable malware detection system using transformers-based transfer learning and multi-model visual representation. Sensors, 22(18), 6766. 2022.*

[18] A.Abbas, M.A. Khan, S. Latif, M. Ajaz, A.A. Shah, J. Ahmad*A new ensemble-based intrusion detection system for internet of things. Arabian Journal for Science and Engineering, 1-15.2021.*

[19] P.R.Saxena, D. Chauhan*EEG Signal Classification using Deep Transfer Learning Technique in an Internet of Medical Things Environment. In 2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing and Communication Engineering (ICATIECE) (pp. 1-6). IEEE.2022.*

[20] A.K. Sahu, S. Sharma,M. Tanveer, R. Raja*Internet of Things attack detection using hybrid Deep Learning Model. Computer Communications, 176, 146-154.2021.*

[21] P. Nimbalkar, D. Kshirsagar*Feature selection for intrusion detection system in Internet-of-Things (IoT). ICT Express, 7(2), 177-181.2021.*

[22] R. Gangula, V, M. M.*Network intrusion detection system for Internet of Things based on enhanced flower pollination algorithm and ensemble classifier. Concurrency and Computation: Practice and Experience, 34(21), e7103.2022.*

[23] Y. Wang, G. Qin, M. Zou, Y. Liang, G. Wang, K. Wang, Z. Zhang*A lightweight intrusion detection system for internet of vehicles based on transfer learning and MobileNetV2 with hyper-parameter optimization. Multimedia Tools and Applications, 1-23..2023.*

[24] D.Y.Mikhail, R.S. Hawezi, S.W. Kareem*An Ensemble Transfer Learning Model for Detecting Stego Images. Appl. Sci. 13, 7021.2023.*

[25] P. H.Q.Awla, S.W.Kareem,A.S. Mohammed*A Comparative Evaluation of Bayesian Networks Structure Learning Using Falcon Optimization Algorithm. International Journal of Interactive Multimedia and Artificial Intelligence, 527.2023.*

[26] F. Hussain, S. G. Abbas, U. U. Fayyaz, G. A. Shah, A. Toqeer and A. Ali*Towards a Universal Features Set for IoT Botnet Attacks Detection," 2020 IEEE 23rd International Multitopic Conference (INMIC), Bahawalpur, Pakistan, 2020, pp. 1-6, 2020.*

[27] T.M. Booij, I. Chiscop,E. Meeuwissen, N. Moustafa, F.T. Den Hartog, *ToN-IoT: The role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets. IEEE Internet of Things Journal,*

9(1), 485-496.2021.

[28] Stratosphere Laboratory. A labeled dataset with malicious and benign IoT network traffic. Agustin Parmisano, Sebastian Garcia, Maria Jose Erquiaga, (accessed April 26, 2020). Online. Available: https://www.stratosphereips.org/datasets-iot23.

Edited by: Mustafa M Matalgah
Special issue on: Synergies of Neural Networks, Neurorobotics, and Brain-Computer Interface Technology: Advancements and Applications
Received: Dec 18, 2023
Accepted: Mar 18, 2024