AN IN-DEPTH EXPLORATION OF CONTEMPORARY APPROACHES FOR DETECTING BOTNET ATTACKS

***Mr.Sandip Y. Bobade** Research Scholar,Computer Engineering Dept, SMT.Kashibai Navale College Of Engineering SPPU,Pune,India sandip.bobade@gmail.com*
***Dr,Ravindra S. Apare** Associate Professor in IT Department,Trinity College of Engineering and Research,SPPU,Pune, ravi.apare@gmail.com*
***Mr. Ravindra H. Borhade** Associate Professor and Head Department of Computer Engineering ,STES Smt. Kashibai Navale,College of Engineering, SPPU, Pune,india rhborhade@gmail.com*

Abstract: The Internet of Things (IoT) is a novel paradigm for communication that uses the internet to connect a wide range of commonplace devices. A new age of clever gadgets that are effortlessly integrated into our daily lives has arrived as a result of its rapid proliferation. Smart homes, smart offices, smart utilities, smart healthcare, intelligent farming, smart transportation, smart villages, and more have all seen creative uses spurred by this game-changing technology. These applications have the ability to significantly improve our quality of life by enabling proactive, self-governing systems that don't require constant human interaction. Additionally, IoT applications and devices have been smoothly incorporated into key infrastructures, which include transportation networks, healthcare facilities, nuclear power plants, water treatment centres, and power plants. Their integration into these crucial areas has resulted in enhanced functioning and accessibility. capabilities for remote management enable. However, at the same time as IoT has becoming widely adopted, major cybersecurity flaws have also been exposed. These weaknesses include passwords that are hardcoded and security setups that aren't up to par. The systemic problems can be attributed to IoT providers' past disregard for strong security protocols. Numerous research projects have proposed machine learning centred methods to detect threats like malware networks and Distributed Denial of Service (DDoS) assaults in response to these security challenges. Interestingly, these methods have demonstrated that applying optimization algorithms can significantly increase machine learning accuracy. Still, there is a constant search for more sophisticated methods, driven by the need to overcome the limitations that come with making mistakes.

Keywords—IoT, Botnet, Machine Learning, Security, DDoS, Hybrid classifier

I. INTRODUCTION

In the internet age we live in, real-world objects are becoming more sophisticated, smart, and able to interact with each other without the need for human intervention in order to improve and enrich human existence. [1] [10, 11, 12, 14, 13, 13]. The idea of the Internet of Things (IoT) is introduced by the connecting of physical things to the World Wide Web. The internet of things (IoT) is an conversation of information paradigm that links a vast array of everyday devices. As the Internet of Things developed, smart gadgets became a part of everyday life. Numerous cutting-edge uses of smart technology, including smart cities, smart offices, smart grids, smart homes, smart transportation, smart agriculture, and smart healthcare, have been transformed by IoT. Our lives is becoming more reliant on smart devices [2]. IoT security remains the primary issue despite this valuable revolution [3]. In order to get their product onto the market and start making more money as soon as possible, IoT companies are concentrating more on enhancing the functionalities of their devices than on making them secure. [4] [12, 15, 16, 17, 18, 18]. Because we use electronic devices so frequently, an IoT security breach could adversely affect our daily life. [19] [20] [21] [22]. In order to improve their efficiency and make them more remotely accessible, key infrastructures such as transportation, healthcare, nuclear, water, and power plants are also using IoT devices and applications. The rising number of internet of things devices being used in critical organizations is also raising the Potential risk of cybersecurity attacks due to the important security problems that IoT devices naturally contain [5] [6] [7] [8] [10] [9]. Therefore, if the Internet of Things (IoT) gadgets and applications are not adequately secured, the attack could have catastrophic impacts on these vital infrastructures. Particularly, several significant cyber-security issues, such as encoded or weak security passwords, inadequate security setups, etc., are passed on through IoT devices [5]. This is a result of IoT supplier insufficient focus on strong safety precautions. [6] [7, 23–24, 25–26, 27]. IoT device security flaws have made it easier for cybercriminals to seize control of Internet of Things devices and use them for nefarious purposes like botnet attacks [8]. Botnets are a network of related, remotely weakened devices containing malware. managed by servers for command and control [1]. The attackers exploit the botnet for malevolent purposes, such as destabilizing a web site with distributed denial of service (DDoS) attacks, sending spam emails, and click fraud. Botnets have been everywhere for a while, but as vulnerable IoT devices increase, they have grown larger, more intricate, and more harmful. These days, botnet attacks pose a major risk to the whole internet [1]. [28, 29, 30, 31,32].The increasing prevalence of unsecured Internet of Things (IoT) devices has made it easier for attackers to take advantage of these devices and integrate them into botnet armies to carry out extensive harmful operations [1] [9]. Numerous publications have up to now proposed different ML driven methods to identify the botnet, Dos attacks, but the dataset they are trained on limits how well they perform. This is due to the fact that while the features utilized for training the machine learning model perform well on a particular botnet dataset, they do not function well on other datasets due to the variety of attack patterns that exist. Given that the training feature set of ML models has a significant impact on their performance [11] [33], selecting the right features is crucial for effective attack detection. In addition, many instances have demonstrated that applying optimization methods can improve machine learning accuracy [10].

II. MOTIVATION

The study of literature survey has helped in identifying the key issues. There exists a wide scope in considering these issues as research opportunities. The description of these motivational factors is mentioned below.Botnets have existed around for more than 20 years, and as the Internet of Things (IoT) has developed, they have grown to more devices than anyone could have predicted, including toasters, refrigerators, printers, and webcams. A portion of botnets use compromised devices to mine cryptocurrencies or obtain credentials from unaffiliated devices.The features and challenges of the most interesting works discussed in literature are shown in Table I. the PSI-rooted subgraph in [1] achieves higher detection rate. But, here the processing time is higher. The Grey Wolf Optimization algorithm utilized in [2] achieves the lowest detection time and achieves best combination of TPR and FPR values Apart from this advantage, the reliability of this technique is lower. Further, the A graph-based strategy yields a higher accuracy rating. But, it suffers from over-fitting problem. Deep Autoencoders in [5] consumes detection time and it consumes lower cost. Moreover, the Detection of Anomalies Based on Graph Structure (GSBDA) utilized in [6] has higher prediction accuracy and lower time complexity. Apart from this advantage, it suffers from lower packet arrival time and packet delivery ratio. Bypass-Linked Attacker Update-based ROA (BAU-ROA) and The Deep Belief Network introduced in [7] has higher throughput and lower latency, which makes it more significant for attack detection. But, the energy consumption during the attack detection is higher. likewise the IC-MADS [8] provides improved protection with the least amount of overhead and energy.. But, this technique suffers from higher communication overhead. In terms of F1-Score and detection rate, the GNN-Based botnet detection system[9] can perform better than the most advanced methods but not consider network communication flow features. Therefore, there is a necessity to develop a override the major drawback of error reduction.

III. LITRATURE RIVIEW

By fusing machine learning and deep learning models, Nguyen et al. [1] introduced a novel high-level PSI-rooted subgraph-based feature for the identification of IoT botnets in 2020. They have created a limited set of features that have precise behavioral definitions, resulting in reduced processing time and space requirements. The efficiency and resilience of Features based on subgraphs rooted in PSI are demonstrated by the k-Nearest Neighbor, Random Forest, Decision Tree, Support Vector Machine and Bagging are the five machine classifiers, which all succeed in achieving a detection rate of more than 97% and reduces time-consuming results. Amina Arshad and associates in 2023 [2] With strong performance scores, the author created an ensemble learning system to identify botnets in network traffic. After analyzing the traffic, the system will look for any unusual activity that would point to the existence of a botnet. They developed the applied machine learning and deep learning approaches for comparison using the benchmark CTU-13 dataset. They suggested a brand-new ensemble method called K-neighbors, Decision tree, and Random Forest (KDR) in order to obtain excellent botnet attack detection performance.2021: Ning Zhang and Tolijan Trajanovski. [3] The IoT-BDA framework, a unique framework for automating the collection, analysis, detection, and reporting of IoT botnets, was created and assessed by the author. The framework comprises of honeypots combined with an innovative sandbox that can detect signs of compromise and assault, as well as anti-analysis, anti-persistency, and anti-forensics methods. It supports a broader variety of software and hardware configurations. These features may improve the efficacy of infection treatment, botnet analysis, and detection. The framework helps with botnet suspension by sending the results to an abuse service and blacklist. The found anti-honeypot strategies and the steps taken to lower the chance of a honeypot being discovered are also detailed in the study. Mu'awya Al-Dalaien and Qasem Abu Al-Haija in 2022. [4] The author presented An ensemble-based learning approach to botnet attack detection called ELBA-IoT in Internet of Things networks. This model use ensemble learning to detect Unusual activity on the network coming from infected IoT devices by profiling behavior aspects of IoT networks. Furthermore, the assessment of three distinct machine learning methods that are part of decision tree methods— RUSBoosted , AdaBoosted , and bagged—is characterized by the IoT-based botnet detection strategy. Shorman et al. [5] created a unused unsupervised evolutionary IoT botnet finding method in 2019. The primary goal of the suggested approach is to identify IoT botnet attacks that originate from compromised IoT devices. To do this, it takes advantage of the effectiveness of a recently developed swarm intelligence algorithm known as the Grey Wolf Optimization technique (GWO) to tune the hyperparameters of the OCSVM while also identifying the characteristics that most accurately characterize the IoT botnet issue. The performance of the recommended method is assessed using standard anomaly detection assessment metrics over an updated version of an actual benchmark dataset in order to demonstrate its efficacy. The experimental findings demonstrate that the suggested strategy beats every other algorithm in relations of G-mean, true positive rate, and false positive rate for all various kinds of IoT devices. In addition, it minimizes the number of carefully chosen features while achieving the fastest detection time. A straightforward technique for detecting Internet of Things botnets was presented by Nguyen et al. [6] in 2019. It is based on the extraction of high-level data from PSI-Graphs, or function-call graphs, for each file that is currently open. This characteristic demonstrates the efficacy in handling multi-architecture problems without requiring the intricate The control flow analysis of graphs, which is necessary for the majority of existing techniques. The outcomes of the experiment demonstrate that the recommended strategy accomplishes a 98.7% correctness rate using a dataset of 11,200 ELF files that includes 4001 normal samples and 7199 IoT malware samples. Furthermore, a comparison with other current approaches shows that our strategy produces superior results. Meidan et al. [7] offered N-BaIoT, the novel anomaly detection method for the IoT based on networks, in 2018. It captures snapshots of network behavior and using deep autoencoders to recognize unusual network data from IoT devices that have been compromised. We used two popular IoT-based botnets, BASHLITE and Mirai, to spread to nine corporate Internet of Things gadgets in our lab in order to assess our methodology. The evaluation's findings showed that our suggested approach could quickly and precisely identify the assaults as soon as they were initiated from the IoT devices that were part of a botnet that were compromised. Asadi et al. [8] employed a combination of the element 2020: BD-PSO-V, a swarm optimization (PSO) method by a voting mechanism to notice botnet occurrences in the IOT. The PSO technique was used to identify exceptional and useful traits for botnet detection. To recognize botnets and categorize samples, the voting system made use of a deep neural network method, SVM and decision tree (C4.5). The most significant novelty of this study was combining the PSO feature selection algorithm through a voting system that used deep learning to classify botnets. The voting system's decision-making technique was built on extreme votes. The Bot-IoT and ISOT datasets were utilized in order to further validate the BD-PSO-V system. execution. Compared to the other approaches tested, the accuracy was enhanced through a means of 0.17% and 0.42% in the BotIoT and ISOT datasets respectively. correspondingly, by using BD-PSO-V simulation. Furthermore, an assessment was conducted on the impact of six prominent adversarial attacks on both datasets. The findings of BD-PSO-V shown a auspicious performance in the face of several threats, though a minor decrease in accuracy rate. A Fresh Forecastive Anomaly based Botnet Revelation Framework was created in 2020 by Bhatt and Thakke [9] to categorize malevolent automated programs and more irregularities in the network. The method is two-step: the primary step is occurrence creation, and the second is classification. In our study, an Ensemble based Stream Mining is employed as another to ML technique to generate multiple instances with less time and memory. After the creation of the instances, the stream mining algorithm's features are used to trigger Graph Structure Based Detection of Anomaly [GSBDA], which looks for potentially dangerous abnormalities. Furthermore, an instance-based learning technique known as the KNN (K Nearest Neighbor) algorithm is employed in the second phase. By watching the network flows, it is utilized to properly identify the Botnet. A unique approach for identifying and averting HELLO flooding attacks through an improved deep learning mechanism was presented by Srinivas et al. [10] in 2020. k-path creation, Cluster head selection, HELLO flooding attack detection, defense, and the best shortest path selection stages were all included in this model. In order to identify and stop the HELLO flood assault, specific Vectors of Route Discovery Frequency, including Each node's route discovery time as well as the inter route discovery time, were set up once the k-paths and cluster head were chosen. First, to determine the stranger node, a threshold value was used to compare each node's estimated RSS. The HELLO flood attack was verified by DBN, and it was ultimately detached from the network. The selection of the shortest path was finished. following network security using the enhanced BAU-ROA meta-heuristic model, and it was used to enhance the best DBN as well. When determining the best shortest path, the objective constraints—such as trust, the distance between nodes, transmission delay, and packet loss ratio—were taken into account. Soe et al. [11] presented a machine learning (ML)-based sequential detection architecture botnet attack detection system in 2020. The growth of an effective, lightweight identification method employs a successful method of feature selection. Botnet attack detection achieves a detection performance of over 99% when three distinct machine learning techniques are used: artificial neural network (ANN), J48 decision tree, and Naïve Bayes. The result of the experiment shows that the suggested architecture has the capability of both successfully identifying botnet-based attacks and expanding with matching sub-engines for novel attack types, A unique comprehensible GNN-Based botnet detection the solution was proposed in 2023 by Wai Weng Lo et al. [12]. They first propose XG-BoT, a botnet detection system which makes use of a graph isomorphism network and the grouped reversible residual connection. Next, by emphasizing fictitious network flows and botnet nodes, GNN Explainer and saliency map were implemented. Two benches were used for the purposes of F1-Score and detection rate based on the testing results. Additionally, identifying the botnet nodes and unusual network flows can help in proactively interpreting botnet patterns for network forensics. Beluga Whale Optimization (BWO) is an innovative metaheuristic algorithm indicated by Changing Zhong et al. [13] in 2022. BWO, which consists of three phases exploration, exploitation, and whale fall—was inspired by the behaviors of beluga whales, including swimming, fishing, and falling prey. BWO is a simple to use, derivative-free optimization method. BWO offers competition for composite functions and performs excellently for single-modal and multimodal functions, particularly in scalability analysis. According to Changjin Yang et al. (2023), the centroid opposition-based learning strategy should be used rather than the first random creation method to enhance the original population generation plan of the Dung Beetle Optimizer

(DBO).. The improved DBO is utilized in the realm of IoT detection of botnets and is used to optimize Catoost settings. Performance comparison experiments are conducted using real-world IoT traffic datasets. Based on the experimental results, the suggested methodology is beneficial in this field since it performs better than other models in terms of accuracy and F1 score.

Table 1. Features and Challenges of existing models

Author &Year	**Methodology**	**Advantages**	**Drawbacks**
The Nguyen group [1][2020]	subgraph rooted in PSI	elevated detection rate	Reduced Fscore
Amina Arshad etal .[2][2023]	Ensemble learning system	solution for securing IoT devices	Need advanced data balancing feature selection techniques
Tolijan trajanovskiand Ningzhang[3][2021]	IoT-BDA	Automatically identifies IoC and IoA and helps	Suffers from over-fitting
Qasem Abu Al-Haija and Mu’awya Al Dalaien. [4][2022]	ELBA-IoT	Higher Detection Accuracy	High memory utilization
Shorman et al. [5][2019]	In The Grey Wolf Optimization algorithm	There is a decent balance between TPR and FPR values	lower rate of false positives
[2019] Nguyen et al.[6]	A graph-based strategy	delivers a higher accuracy rating.	Experiences overfitting.
Meidan and associates. [7][2018]	Deep Autoencoders	Reduced time of detecting	Increased complexity of computation

Asadi & Co. [8][2020]	Voting System-Based Particle Swarm Optimization Algorithm	high rate of detection and accuracy	Reduced reliability
Thakke and Bhatt [9][2020]	Dependent Identification of Variations on Graph Structure	exceptional accuracy in predicting	Greater packet loss
Srinivas *et al.* [10] [2020]	(DBN) and (BAU-ROA	reduced latency	Greater energy consumption
Soe *et al.* [11] [2020]	IC-MADS	Better protection is achieved with IC-MADS while consuming the least amount of overhead and energy	decreased effectiveness in terms of energy No performance exchange greater communication overhead
Wai Weng Lo et al.[12] [2023]	GNN-Based botnet detection system XG-BoT	Achieve better F1-Score and detection rate	Lower efficient on edge-based graph encoders
Changting Zhong	Optimization of	Capability to balance	not solve discrete problems.

et al. [13] [2022]	Beluga whales An innovative metaheuristic algorithm inspired by nature	the exploration and exploitation phase exceptional for scalability study,	
Yang, C,et al. [14] [2023]	(DBO), which use the centroid opposition-based learning approach	beats alternative models in terms of F1 score and accuracy.	limitations when dealing with imbalanced data ,need to focus on minority class

Table 2. Feature Selection Technique and Dataset

Author and year	**Feature selection method**	**Dataset**	**Advantage**
Mnahi Alqahtani *,et al[1][2020]	Using a genetic-based extreme gradient boosting (GXGBoost) mode in conjunction with a feature selection method based on Fisher scores	(N-BaIoT) dataset	high detection rate
Mohammed Al-Sarem et al[40] [2021]	Mutual Information (MI) method, ANOVA f-test at the finely-granulated detection level, and Principal Component Analysis (PCA)	(N-BaIoT) dataset	The strategy based on MI filters produced the best accuracy score when applied to binary datasets.
Xiangyu Liu and Yanhui Du [41][2023]	genetic algorithm-based feature selection technique.	(N-BaIoT) dataset	Less training time and high accuracy
Arvind Prasad et al[42]2023	Four distinct methods were used: correlation into FISet, CorSet, MISet, and LassoSet;feature importance's mutual_info_clasif; and the selection operator with the least absolute shrinkage (LASSO).	UNSW CICIDS2018 UNSW NB15 BoT IoT 2018 Live Traffic	Early detection of bots,

IV PROPOSED SYSTEM

Our lives are now impacted by IoT gadgets. New threat models are also expected to emerge as a result of the internet's expanded reach. One of these risks that can affect IoT devices is the IoT botnet. There are numerous ways to find these kinds of attacks. Although these techniques work well, there are still certain issues with detecting accuracy. Thus, based on an enhanced hybrid model of classification, a unique the Internet of Things botnet identification technique is presented In this research endeavor. The two main stages of the proposed study are attack detection and feature extraction. Fig. 1 depicts the architecture of the suggested project. The first features to be retrieved are the flow-based features, enhanced correlation-based features, and higher order statistical features. The attack detection process then occurs the retrieved features will be used to train the hybrid classifier. Moreover, The combination of the two will result in the hybrid classifier. the Recurrent Neural Network (RNN) with the Improved Deep Belief Network (DBN), in that order. Self-adaptive Beluga whale optimization will be applied in order to adjust the RNN weight. in order to increase the IoT botnet accuracy for detection. In actuality, the BBMO [34] is a brand-new algorithm inspired by nature that solves global unconstrained optimization problems by simulating bumblebee mating behavior. The hybrid's ultimate product classifier portrays about whether or not there is an IoT botnet attack.

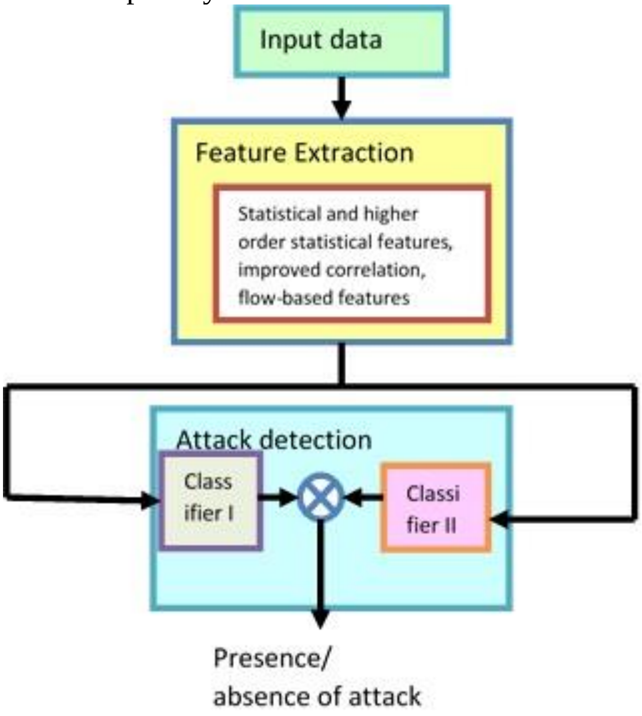

Input data
Feature Extraction
Statistical and higher order statistical features, improved correlation, flow-based features
Attack detection
Class ifier I
Classi fier II
Presence/ absence of attack

Figure 1: Working Principle of Proposed Model

V.Experimental results and discussion

A number of tests were conducted utilizing the suggested data sources to evaluate the effectiveness and performance of the DT, NB, ANN, and ensem-ble approach for detecting harmful events. The evaluation measures of accuracy, False Positive Rate (FPR), Detection Rate (DR), and ROC curves are utilized to do this. The four terms True Positive (TP), True Negative (TN), False Negative (FN), and False Positive (FP) are the foundation of these measures. TP is the total amount of anomalous records that have been found to be attacks.

Table 3 : A comparative summary of evaluation performance on the UNSW-NB15 dataset

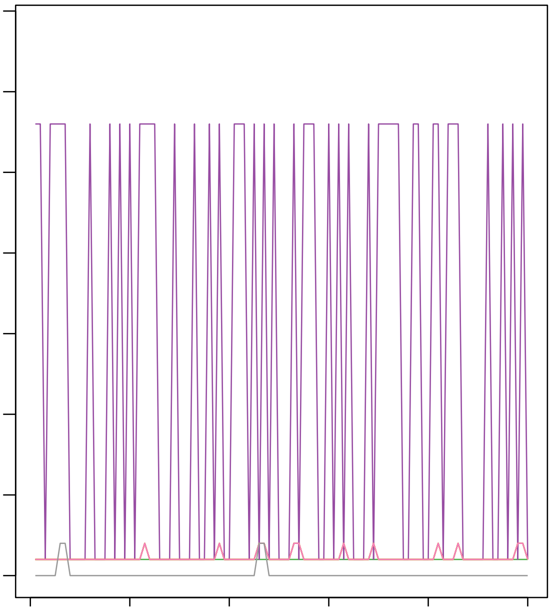
Alg.	**DNS data source**				**HTTP data source**			
	Acc (%)	**DR (%)**	**FPR (%)**	**Time Sec**	**Acc (%)**	**DR (%)**	**FPR (%)**	**Time Sec**
DT	95.32	94.15	5.22	125.3	97.13	96.34	3.43	124.3
NB	91.17	90.78	8.25	130.2	95.91	95.25	4.18	131.1
ANN	92.61	91.48	7.87	220.2	96.27	95.53	4.26	217.2
Ensemble	99.54	98.93	1.38	150.8	98.97	97.02	2.58	148.3

Table 4 : Assessment results on the NIMS dataset: A comparative overview

Alg.	DNS data source				HTTP data source			
	Acc (%)	DR (%)	FPR (%)	Time Sec	Acc (%)	DR (%)	FPR (%)	Time Sec
DT	96.10	95.02	4.19	128.5	97.23	95.92	4.65	129.6
NB	88.28	87.15	11.15	126.4	93.83	92.19	6.87	125.3
ANN	94.22	93.47	6.76	216.7	95.52	94.34	5.13	209.1
Ensemble	98.29	97.38	2.01	142.1	98.36	97.95	2.15	145.5

VI.EVALUATION AND DISCUSSION

Normal DNS data



Attack DNS data

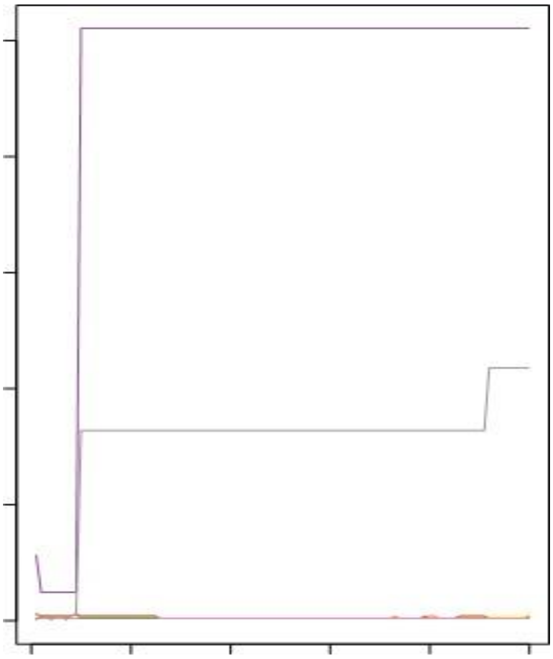
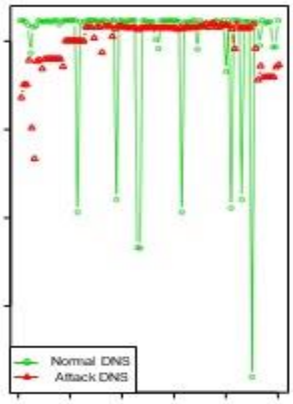


Figure. 2. Dissimilarity of normal and attack DNS instances

Correntropy of DNS instances



Correntropy of HTTP instance

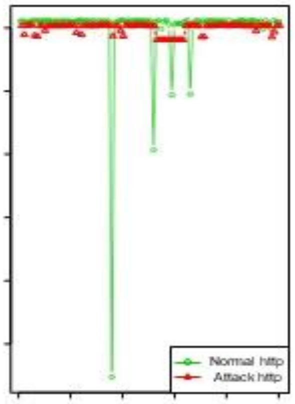


Table 5: Comparing DRs (%) and FPRs (%) using the ensemble approach

Record types	DNS data source		HTTP data source	
	DR	FPR	DR	FPR
Normal	97.53	0.24	99.01	0.15
DoS	98.22	0.31	98.54	0.42
Exploits	96.57	0.52	95.25	0.57
Fuzzers	99.86	0.01	99.23	0.02
Generic	99.43	0.13	96.63	0.72
Reconnaissance	99.78	0.04	98.57	0.24
Analysis	-	-	99.20	0.38
Backdoor	-	-	95.25	0.61
Worms	-	-	99.62	0.05

The DNS and HTTP data sources of the UNSW-NB15 and NIMS botnet datasets, as shown in Tables 4 and 5, respectively, are used to evaluate the overall performance of the DT, NB, ANN, and the proposed ensemble technique in terms of Accuracy (Acc), DR, FPR, and processing time (Time). On the one hand, the accuracy and DR of the ensemble method obtain 99.54% and 98.93%, respectively, using the DNS data source of the UNSW-NB15 dataset; on the other hand, the FPR yields 1.38%, which surpasses the performance of the DT, NB, and ANN techniques. The ANN approach achieves a 92.61% accuracy, 91.48% DR, and 7.87% FPR, whereas the DT strategy yields a 95.32% accuracy, 94.15% DR, and 5.22% FPR. Finally, the accuracy rate of the NB approach is attained. of 8.25% FPR, 90.78% DR, and 91.17%. The ensemble method is ranked as a second technique when compared to the other methods, taking an average of 150.8 seconds for 200,000–300,000 samples. While this approach occasionally requires computational resources, the AdaBoost approach can send the data to any method that performs a better job of appropriately classifying abnormal behaviour's.

VII.CONCLUSION

The proposed IoT botnet attack detection model will be implemented in PYTHON and the experimental investigation will be carried out. The performance analysis will be done by comparing the proposed model over several state-of-the-art models, through the Type 1 measures and Type 2 measures. Here, This research builds an effective network intrusion detection system (NIDS) for detecting attacks that exploit Internet of Things (IoT) networks by identifying a collection of attributes from a detailed investigation of the TCP/IP architecture, particularly the MQTT, DNS, and HTTP protocols and their flow IDs. The suggested group structure is examined. In order to increase overall performance in terms of accuracy, detection rate, and processing time when compared to various state-of-the-art approaches, an AdaBoost ensemble method utilizing three techniques—DT, NB, and ANN—was implemented. support the use of the suggested ensemble method to identify both current and zero-day attacks.

VIII.REFERENCES

[1] Huy-Trung Nguyen, Quoc-Dung Ngo, Doan-Hieu Nguyen, Van-Hoang Le,"PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms", ICT Express, 2020

[2] Amina Arshad, Maira Jabeen, Saqib Ubaid, Ali Raza, Laith Abualigah, Khaled Aldiabat, Heming Jia, "A novel ensemble method for enhancing Internet of Things device security against botnet attacks", Decision Analytics Journal vol.8, 2023.

[3] TOLIJAN TRAJANOVSKI AND NING ZHANG, "An Automated and Comprehensive Framework for IoT Botnet Detection and Analysis (IoT-BDA)," in IEEE Access, vol. 9, pp. 124360-124383, 2021.

[4] Qasem Abu Al-Haija and Mu'awya Al-Dala'ien, "ELBA-IoT: an ensemble learning model for botnet attack detection in IoT networks", Journal of Sensor and Actuator Networks, vol.11, p.18, 2022.

[5] Amaal Al Shorman, Hossam Faris, Ibrahim Aljarah,"Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection", Journal of Ambient Intelligence and Humanized Computing, 2019

[6] Huy-Trung Nguyen, Quoc-Dung Ngo, Van-Hoang Le," A novel graph-based approach for IoT botnet detection", International Journal of Information Security, 2019

[7] Yair Meidan, Michael Bohadana , Yael Mathov , Yisroel Mirsky, Asaf Shabtai , Dominik Breitenbacher and Yuval Elovici,"N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders", IEEE Pervasive Computing, 2018

[8] Mehdi Asadi,Mohammad Ali Jabraeil Jamali, Saeed Parsa,Vahid Majidnezhad,"Detecting Botnet by Using Particle Swarm Optimization Algorithm Based on Voting System", FUTURE 5424, 2020

[9] Priyang Bhatt and Bhaskar Thakker,"A Novel Forecastive Anomaly Based Botnet Revelation Framework for Competing Concerns in Internet of Things", JOURNAL OF APPLIED SECURITY RESEARCH, 2020

[10] T. Aditya Sai Srinivas, S.S. Manivannan,"Prev ention of hello flood attack in IoT using combination of deep learning with improved rider optimization algorithm", Computer Communications, 2020

[11] Yan Naung Soe, Yaokai Feng, Paulus Insap Santosa, Rudy Hartanto and Kouichi Sakurai,"Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture", Sensors 2020,

[12] Wai Weng Loa,∗∗, Gayan Kulatillekea , Mohanad Sarhana , Siamak Layeghya , Marius Portmanna , "XG-BoT: An Explainable Deep Graph Neural Network for Botnet Detection and Forensics", a School of ITEE, The University of Queensland, Brisbane, Australia arXiv:2207.09088v5 [cs.CR] 11 Mar 2023

[13] Changting Zhong, GangLi, ZengMeng, " Beluga whale optimization: A novel nature-inspired metaheuristic algorithm", Knowledge-Based Systems, vol. 251, September 2022.

[14] Changjin Yang 1 , Weili Guan 2,* and Zhijie Fang 3," IoT Botnet Attack Detection Model Based on DBO-Catboost" Appl. Sci.2023, 13, 7169. https://doi.org/ 10.3390/app13127169

[15] L. Yin, X. Luo, C. Zhu, L. Wang, Z. Xu and H. Lu, "ConnSpoiler: Disrupting C&C Communication of IoT-Based Botnet Through Fast Detection of Anomalous Domain Queries," IEEE *Transactions on Industrial Informatics*, vol.16, no. 2, pp. 1373-1384, Feb. 2020.doi: 10.1109/TII.2019.2940742

[16] H. Xia, L. Li, X. Cheng, X. Cheng and T. Qiu,
"Modeling and Analysis Botnet Propagation in Social Internet of Things," IEEE *Internet of Things Journal*, vol. 7,no.8,pp.7470-7481,Aug.2020.doi: 10.1109/JIOT.2020.2984662

[17] N. Koroniotis, N. Moustafa and E. Sitnikova, "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions," IEEE *Access*,vol.7,pp.61764-61785,2019.
doi: 10.1109/ACCESS.2019.2916717

[18] A. Mahboubi, S. Camtepe and K. Ansari, "Stochastic Modeling of IoT Botnet Spread: A Short Survey on Mobile Malware Spread Modeling," IEEE *Access*, vol. 8, pp.228818-228830,2020.doi: 10.1109/ACCESS.2020.3044277

[19] M. J. Farooq and Q. Zhu, "Modeling, Analysis, and Mitigation of Dynamic Botnet Formation in Wireless IoT Networks," IEEE *Transactions on Information Forensics and Security*, vol. 14, no. 9, pp. 2412-2426, Sept. 2019.
doi: 10.1109/TIFS.2019.2898817

[20] I.Ali *et al.*,"Systematic Literature Review on IoT-Based Botnet,Attack",IEEE*Access*,vol.8,pp.212220-212232,2020.doi:10.1109ACCESS.2020.339985

[21] N. Moustafa, B. Turnbull and K. R. Choo, "An Ensemble Intrusion Detection Technique Based on Proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things," IEEE *Internet of Things Journal*, vol. 6, no. 3, pp. 4815-4830, June 2019.doi: 10.1109/JIOT.2018.2871719

[22] R. Vinayakumar, M. Alazab, S. Srinivasan, Q. Pham, S. K. Padannayil and K. Simran, "A Visualized Botnet Detection System Based Deep Learning for the Internet of Things Networks of Smart Cities," IEEE *Transactions on Industry Applications*, vol. 56, no. 4, pp. 4436-4456, July-Aug.2020.doi: 10.1109/TIA.2020.297 1952

[23] W. Zhang, B. Zhang, Y. Zhou, H. He and Z. Ding, "An IoT Honeynet Based on Multiport Honeypots for Capturing IoT Attacks," IEEE *Internet of Things Journal*,vol.7,no.5, pp. 3991-3999, May 2020. doi: 10.1109/JIOT.2019.2956173

[24] K. Huang, L. Yang, X. Yang, Y. Xiang and Y. Y. Tang, "A Low-Cost Distributed Denial-of-Service Attack Architecture," IEEE *Access*, vol. 8, pp. 42111-42119, 2020.doi: 10.1109/ACCESS.2020.2977112

[25] M. Safaei Pour, S.Torabi,E.Bou-Harb,C.Assi and M. Debbabi,"Stochastic Modeling,Analysis and Investigation of IoT-Generated Internet Scanning Activities," IEEE *Networking Letters*, vol. 2, no. 3, pp. 159-163, Sept. 2020.doi: 10.1109/LNET.2020.2998045

[26] Y. Jia, F. Zhong, A. Alrawais, B. Gong and X. Cheng, "FlowGuard: An Intelligent Edge Defense Mechanism Against IoT DDoS Attacks," IEEE *Internet of Things Journal*, vol. 7, no. 10, pp. 9552-9562, Oct. 2020.
doi: 10.1109/JIOT.2020.2993782

[27] M. Wazid, A. K. Das, J. J. P. C. Rodrigues, S. Shetty and Y. Park, "IoMT Malware Detection Approaches: Analysis and Research Challenges," IEEE *Access*, vol. 7, pp. 182459-182476, 2019.doi:

[28] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," IEEE *Communications Surveys & Tutorials*,vol. 21,no.2,pp.1636-1675,Secondquarter2019.doi: 10.1109/COMST.2018.2874978

[29] O. Shwartz, Y. Mathov, M. Bohadana, Y. Elovici and Y. Oren, "Reverse Engineering IoT Devices: Effective Techniques and Methods," IEEE *Internet of Things Journal*, vol. 5, no. 6, pp. 4965-4976, Dec. 2018.
doi: 10.1109/JIOT.2018.2875240

[30] T. Zhi, Y. Liu and J. Wu, "A Reputation Value-Based Early Detection Mechanism Against the Consumer-Provider Collusive Attack in Information-Centric IoT," IEEE *Access*, vol. 8, pp. 38262-38275, 2020.
doi: 10.1109/ACCESS.2020.2976141

[31] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," IEEE *Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671-2701,thirdquarter2019.doi: 10.1109/COMST.2019.2896380

[32] G. Rosenth,al, O. E. Kdosha, K. Cohen, A. Freund, A. Bartik and A. Ron, "ARBA: Anomaly and Reputation Based Approach for Detecting Infected IoT Devices," IEEE *Access*, vol. 8, pp. 145751-145767, 2020.doi: 10.1109/ACCESS.2020.3014619

[33] T. Mahjabin, Y. Xiao, T. Li and C. L. P. Chen, "Load Distributed and Benign-Bot Mitigation Methods for IoT DNS Flood Attacks," IEEE *Internet of Things Journal*, vol.7,no.2,pp.986-1000,Feb.2020. doi:10.1109/JIOT.2019.2947659

[34] R. Chaudhary, G. S. Aujla, N. Kumar and S. Zeadally, "Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," IEEE *Internet of Things Journal*, vol. 6, no. 3, pp. 4897-4909, June 2019.doi: 10.1109/JIOT.2018.2878707

[35] S. Manimurugan, S. Al-Mutairi, M. M. Aborokbah, N. Chilamkurti, S. Ganesan and R. Patan, "Effective Attack Detection in Internet of Medical Things Smart Environment Using a Deep Belief Neural Network," IEEE *Access*,vol.8,pp.77396-77404,2020.
doi: 10.1109/ACCESS.2020.2986013

[36] J. Habibi, D. Midi, A. Mudgerikar and E. Bertino, "Heimdall: Mitigating the Internet of Insecure Things," IEEE *Internet of Things Journal*, vol. 4, no. 4, pp. 968-978, Aug. 2017.doi: 10.1109/JIOT.2017.2704093

[37] Gong, D.; Liu, Y. A Mechine Learning Approach for Botnet Detection Using LightGBM. In Proceedings of the 2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA), Changchun, China, 20–22 May 2022; IEEE: Piscataway, NJ, USA, 2022; pp. 829–833.

[38] Jiyeon Kim 1,2, Minsun Shim 3, Seungah Hong 3, Yulim Shin 3 and Eunjung Choi 2,3 1"Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning" Appl. Sci. 2020, 10, 7009; doi:10.3390/app10197009 www.mdpi.com/journal/applsci

[39] Deng, Y.; Jiang, H.; Wu, J.; Luo, W. IoT Botnet Detection Based on Graph Neural Networks. J. Wuhan Univ. (Eng. Sci. Ed.) 2023, 56, 371–378