Proceedings of the 7th International Conference on Communication and Electronics Systems (ICCES 2022)
DVD Part Number: CFP22AWO-DVD; ISBN: 978-1-6654-9633-9

Building NIDS for IoT Network using Ensemble Approach

Sivasankari. N
Department of Computer Science
Vels Institute of Science, Technology & Advanced Studies
Chennai, India
sivasankari1985.n@gmail.com

Kamalakkannan. S
Department of Information Technology
Vels Institute of Science, Technology & Advanced Studies
Chennai, India
kannan.scs@velsuniv.ac.in

Abstract- **The term 'IoT' is a trendy word in current era due to its usage in day-to-day life of human beings. Its applications are widespread across many areas such as home, agriculture, health care, transportation, etc., Due to the vast development of IoT services, cyber-attacks against IoT application and devices also increased. Thus, Security and Privacy are concern as two major issues in IoT environment. Building a Network Intrusion Detection System (NIDS) is one of the ways for securing the IoT system against cyber-attacks. So, we proposed an Ensemble based Network Intrusion Detection System using machine learning algorithms to detect botnet attacks against HTTP and DNS protocol in network traffic. The goal of this proposed work is to higher the detection rate and decrementing the false positive rate. UNSW_NB15 dataset was used for evaluating the performance of the proposed NIDS. In this work, an IoT environment architecture using fog node proposed and the performance of various classifiers included in the framework compared with the ensemble method based on detection rate and false positive rate.**

Keywords- Internet of Things (IoT), Network Intrusion Detection System (NIDS), Botnet attack, Ensemble Learning

I. INTRODUCTION

Internet of Things is an interconnection of physical devices which communicate with each other and provide services to the human lives without the intervention of humans. IoT System are extremely significant in many application domains such as home automation, healthcare, vehicle automation, environmental monitoring, manufacturing process, agriculture, logistic, etc., IoT system usually detects the surrounding and gather the data using sensors and actuators; Then the collected information transferred to the server or cloud environment for processing and storing due to the limitation of resource capability in IoT devices. Thus, many IoT applications are depending on cloud computing for processing and storage.

IoT applications uses variety of protocols for performing its basic services but Hyper Text Transfer Protocol (HTTP) and Domain Name Server (DNS) are the most widely used ones. DNS is a hierarchical domain name server in a distributed fashion which provides the conversion from host name to IP address and resolves the contraction among the reserved domain names. HTTP is a client-server protocol and the basic for any data transfer or fetching the resources on the web.

Botnet is one the cyber-attacks which intentionally exploits the data or infrastructure of the target users via protocols using various exploitation techniques. The main worry in IoT system is to safeguard the devices and information from the intruders; thus, lots of personal data are transmitted over the internet.

Network Intrusion Detection System generally utilized for checking and identifying abnormal activities in network traffic [1]. A classic NIDS includes four stages as depicts in fig 1.

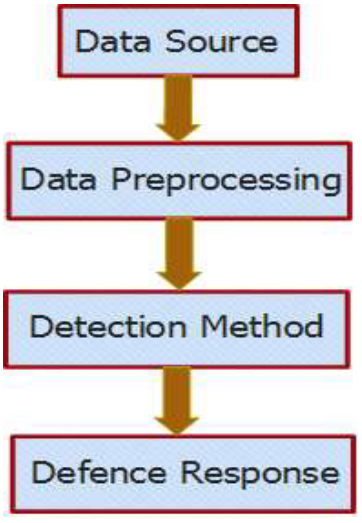

Fig.1. Stages of NIDS

- Data Source contains a list of observations of network traffic, with necessary features

for differentiating authorized and mistrust observations.

- Data preprocessing is a stage were identifying and removal of irrelevant features from the data source
- A detection method uses various classification techniques to predict the traffic as normal or attack
- A defense response is a decision taken to forestall assault activities.

The classic NIDS will not suit for IoT network because it identifies the conventional anomalies in the network traffic. But, the traffic pattern of IoT network will differ from the conventional network. Thus, building a NIDS specific to IoT traffic helps to ensure enhanced protection over IoT networks from the intruders. To protect the IoT system from the attackers, this paper proposes a Network based Intrusion Detection System using ensemble-based approach to detect the attack in the IoT network traffic.

The key contribution of the paper is as follows:

1) Decision Tree (DT), Support Vector Machine and Naïve Bayes (NB) were the Supervised Machine Learning algorithms used in the proposed ensemble learning framework to find the attack.
2) HTTP and DNS based traffic from the dataset is filtered using Extraction module.
3) Relevance analysis performed and adopted correlation-based feature selection for finding relevant features for detecting the attack in HTTP and DNS protocol
4) The performance of the ensemble approach with each classification techniques included in the framework was evaluated using UNSW_NB 15 dataset.

Remaining paper organized as follows: Section II discusses the similar work corresponding to our work. Section III explains the proposed ensemble-based NIDS, Section IV presents the results and discussion of the proposed work and Section V provides the conclusion.

II. RELATED WORKS

The focus of this paper is to build a NIDS to detect the abnormal symptoms of network traffic that exploits or degrades the IoT systems in HTTP and DNS protocol. To improve the overall performance of NIDS, many researchers have undergone based on ensemble method. The previous study related to the paper is as follows:

Vivekanandam [2] proposed a technique to detect the intrusion using hybrid approach of genetic algorithms. But the proposed solve the real-life problem in android categorization. Giacinto. et al [3] proposed a technique to detect multiple types of attacks using ensemble method. But the attack detection decision finally depends on the voting rule method. Bayesian network-based ensemble method was proposed by Chebrolu et al. [4] where classification and regression trees used to identify suspicious instances. When comparing the performance of hybrid/ensemble with each one individually, the hybrid/ensemble provides better performance even though increase in computational overhead. For detecting multiclass attack, Dewan Md. Farid et al. [5] proposed hybrid IDS using decision tree and naïve bayes. Yan Naung Soe [6] proposed botnet attack detection using machine learning technique with sequential architecture, but normal traffic patterns are not investigated to identify the unknown attacks. Mohammad Shorfuzzaman [7] proposed a tree-based ensemble and feedforward neural network to detect unexpected cyber-attacks in IoT but placement strategy of NIDS is not focused.

In this paper, we provide a Network Intrusion Detection System to detect the cyber-attacks possible through HTTP and DNS protocol and to ensure high detection rate in identifying attacks. An NIDS is designed to be implemented in fog node, and thus it provides better security to an IoT environment.

III. PROPOSED ENSEMBLE-BASED NIDS FOR IOT SYSTEM

An Ensemble-based NIDS were proposed to detect the malicious activities in IoT network traffic via HTTP and DNS protocol to protect the IoT system against botnet attacks. The NIDS will not fit directly into IoT devices due to its small size and low computational power[8]. So, this proposed system focused on placing a fog node as a central controller of IoT devices where NIDS houses and thus all the traffic between the IoT end nodes and application server are by passed via fog node. Thus, NIDS in the fog node monitors the traffic to detect anomalies. The proposed IoT environment architecture for placement of NIDS depicted in Fig.2. It shows traffic between an End node at IoT end device layer and application services resides in cloud server are by passed via a fog node. Fog node act as an intermediate between the end devices and application services where NIDS housed and observe the network traffic continuously and detect the malicious attack.

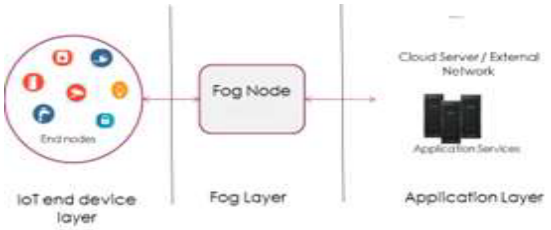

Fig.2. Proposed IoT Environment Architecture using Fog Node

A proposed Ensemble-based NIDS presented in Fig.3 consists of three main steps: Extraction of HTTP and DNS traffic, feature selection and ensemble method. The main idea of the proposed work is to identify the abnormal network traffic to detect the attacks against HTTP and DNS protocol. So, as a first step, traffic based on HTTP and DNS protocols extracted from the UNSW_NB15 dataset. Secondly, Correlation based feature Selection were used to extract the features which have the capability of identifying the legal and malicious pattern. Finally, the ensemble-based technique is implemented based on Bootstrap aggregating using Decision Tree, Support Vector Machine and Naïve Bayes techniques for classifying the traffic as normal or malicious.

A. Feature Selection Method

For NIDS implementation, Feature Selection plays a vital role to identify the essential features which helps to assists in fastidious normal and malicious instances. Thus, performing feature selection removes attribute redundancy, provides better accuracy, and upgrades the performance of NIDS. In this work, correlation-based feature selection is employed to compute the strength between the attributes. The lowest N ranked attributes passed to the ensemble approach for identifying the HTTP and DNS traffic having abnormal activities.

The correlation(R) between feature F1 and F2 calculated by

$$R(F1,F2) = \frac{\sum_{i=1}^{n}(x_i-\overline{F1})(y_i-\overline{F2})}{\sqrt{\sum_{i=1}^{n}(x_i-\overline{F1})^2\sum_{i=1}^{n}(y_i-\overline{F2})^2}} \quad (1)$$

$$\overline{F1} = \left[\frac{\sum_{i=1}^{n}x_i}{n}\right];\ \overline{F2} = \left[\frac{\sum_{i=1}^{n}y_i}{n}\right] \quad (2)$$

The output of R varies in a range between -1 and +1. If the R value is close to +1, it refers there exists a strongest correlation between F1 and F2 and trends of both the features are in same direction. If R value moving neared to -1, it indicates the strongest correlation between F1 and F2 but the features trends are in opposite direction.

B. Supervised Machine Learning Techniques

Supervised machine learning techniques such as DT, SVM and NBare used in this proposed work to implement an ensemble method with bootstrap aggregating to classify the instances as normal and malicious.

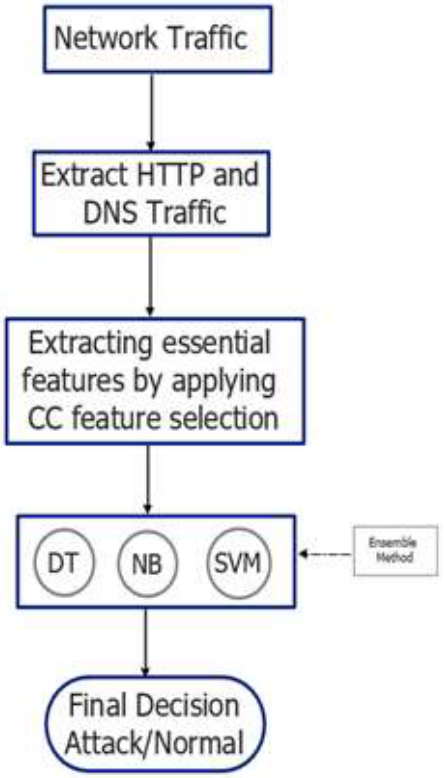

Fig.3. Proposed Ensemble Framework

The machine learning techniques DT, NB and SVM chosen due to its efficiency in classifying legitimate and suspicious vectors with small variations. The three techniques used in the ensemble-based NIDS described briefly below.

1) Decision Tree (DT): It is a tree based structural techniques used for classification problem. Internal nodes of the tree contain test conditions for features to separate instances that have dissimilar characteristics. The C4.5 DT method is used for implementation due to its simplicity. In the training phase, information gain principle is adopted for splitting the samples into subsets. The final decision of choosing the splitting attribute is based on value of gain ratio. Attributes having highest value for gain ratio is selected.

2) Naïve Bayes (NB): NB algorithm solves the classification problem and identifies the categorial label based on Bayes theorem to find the maximal likelihood hypothesis. It suited for high dimensionality dataset and makes quick prediction based on the probability of an object. The posterior

function used to predict the data objects is computed by

$$P(C|I) = argmax_{w\in\{1,2,....N\}} P(C_w) \prod_{j=1}^{N} P(I_j|C_w) \quad (3)$$

3) Support Vector Machine (SVM): In SVM, training data reworked into better dimension using nonlinear mapping. Then it finds the linear hyperplane that separates the instances of one class from other. SVM chooses the extreme vectors to create the 'decision boundary'. Let the Dataset D have set of instances Xi, each associated with the class label yi.Each value of yi can be -1 or +1.

C. Bootstrap Aggregator

In the proposed work, bootstrap aggregator method used to achieve ensemble-based classifier. After important attributes extracted using coefficient Correlation from the dataset, network traffic distributed to the machine learning techniques, Bootstrap aggregator model used. Each classifier Model Mi included in the work return its predicted value for new instance, X. The Bagging model counts the vote of each classifier and assigns the label with the foremost votes to X.

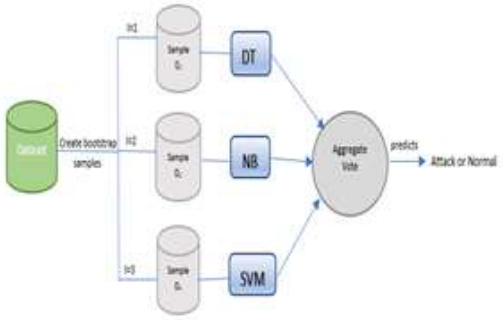

Fig.4. Bootstrap Aggregator Flowchart

IV. RESULTS AND DISCUSSION

This section demonstrates the UNSW_NB15 dataset and performance evaluation metrics used in the proposed work. Then, the findings of ensemble learning framework illustrated.

A. Dataset

The proposed framework is illustrated using UNSW_NB15[9,10] dataset. This dataset contains several forms of data for evaluating NIDS. The focus of our work is to detect attacks against HTTP and DNS protocols. The CSV files of HTTP and DNS data traffic classified into eight different botnet attacks. It includes Backdoor, DoS, Analysis, Exploits, Fuzzer, Generic, Reconnaissance and worm.

UNSW_NB15 dataset includes 68661 DNS traffic instances and 27011 HTTP traffic instances. Table 1 gives the distribution of normal and attack instances based on different categories of botnet attacks.

TABLE I. ATTACK TYPES IN DATA SOURCE

Attack Types	DNS data	HTTP data
Analysis	0	558
Backdoor	0	92
DoS	147	1709
Exploits	253	11481
Fuzzers	375	1087
Generic	57278	502
Reconnaissance	47	2073
Worms	0	148
Normal	10561	9361

B. Performance evaluation Metrics

The efficiency and performance of the ensemble method are analyzed by several experiments using the UNSW_NB15 data source. The metrics such as Accuracy, Detection Rate (DR) or True Positive Rate(TPR), False Positive Rate(FPR) and Precision rate are used to evaluate the performance of ensemble classifier and each classifier included in the framework.True Positive (TP) rate refers the attacks correctly predicted as attacks, True Negative (TN) rate refers the normal traffic predicted correctly as normal, False Positive (FP) refers the wrong identification of non-attack traffic as malicious, False Negative (FN) refers the wrong identification of attack as non-attack, where Actual Positive and Actual Negative represents the actual number attack and non-attack observations.The metrics used in the evaluation is briefly described below.

1) Accuracy: It estimates the percentage of observations that are correctly predicted as normal and attacks, given by

$$\text{Accuracy} = \frac{TP+TN}{Total\ observations} X100 \quad (4)$$

2) Detection Rate (DR): It gives the percentage of observation correctly identified as attacks among the total number of attack instances.

$$\text{DR} = \frac{TP}{Actual\ Positive} X\ 100 \quad (5)$$

3) False Positive Rate (FPR): It gives the percentage of observation incorrectly classified as

attacks among the total number of non-attacks instances

$$\text{FPR} = \frac{FP}{Actual\ Negative} X100 \quad (6)$$

C. Evaluation and Discussion

From the UNSW_NB15 datasets, the instances are extracted as two separate CSV file based on application layer protocol, HTTP and DNS. Then, CC is used for identifying the essential features from the dataset for predicting the attacks. Finally, the ensemble-based NIDS framework performance is evaluated on the two data source. Python is used for implementation on Window 10 Operating system 8 GB RAM and an i7 processor.

The performance of DT, SVM, NB and ensemble approach in measures of accuracy, DR, FPR is demonstrated in Table II and III. Using DNS source, the proposed ensemble technique produces 97.77% accuracy and DR at 97.57%, while the FPR is 2% which is better than the performance of DT, SVM and NB techniques. The DT classifier achieves 90.73% accuracy, 87.4% DR and 5.7% FPR, then the NB classifier produces 93.24% accuracy, 91.41% DR and 4.8% FPR. Finally, the SVM techniques produces 96.42 % accuracy, 95.7% DR and 2.8% FPR.

TABLE II. PERFORMANCE EVALUATION OF DNS DATA SOURCE

Algorithm	DNS Data Source		
	Acc (%)	DR (%)	FPR (%)
DT	90.73	87.4	5.7
NB	93.24	91.41	4.8
SVM	96.42	95.7	2.8
Ensemble	97.77	97.57	2.0

TABLE III. PERFORMANCE EVALUATION OF HTTP DATA SOURCE

Algorithm	HTTP Data Source		
	Acc(%)	DR(%)	FPR(%)
DT	96.75	97.41	6.7
NB	99.3	99.46	1.5
SVM	97.56	98.41	6.9
Ensemble	99.56	99.73	1.3

Using the HTTP data source, the proposed ensemble technique produces 99.56% accuracy and DR at 99.73%, while the FPR is 1.3%. The DT classifier achieves 96.75% accuracy, 97.41% DR and 6.7% FPR, then the NB classifier produces 99.3% accuracy, 99.46% DR and 1.5% FPR. Finally, the SVM techniques produces 97.56 % accuracy, 98.41% DR and 6.9% FPR. In HTTP data source also, the ensemble approach produces better outcomes when compared with the performance of other three techniques included in the framework

From the Fig 5 and 6, it is clearly shown that the proposed ensemble method detects the attacks more effectively compared with DT, NB and SVM. Positive Rate.

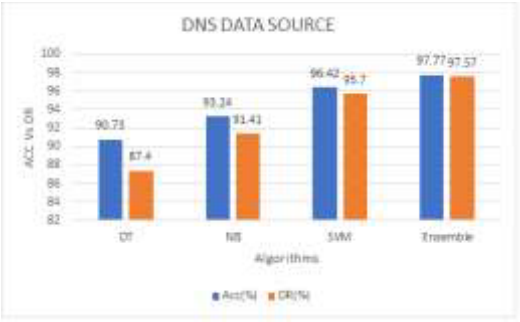

Fig.5. Performance measures of DNS data source

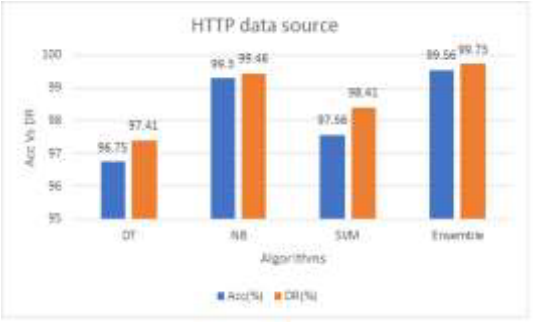

Fig.6. Performance measures of HTTP data Source

Fig.7 shows the False Positive Rate of proposed ensemble method against DT, NB and SVM. The ensemble method produces a lower false positive rate for both the data sources compared with other techniques.

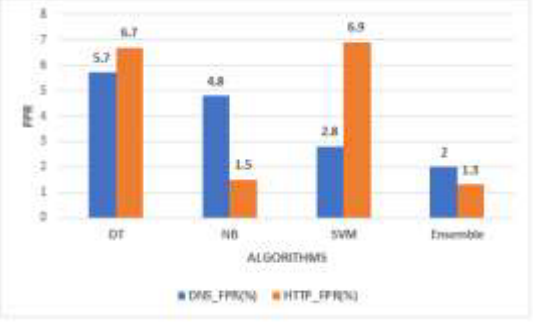

Fig.7. False Positive Rate of HTTP and DNS

V. CONCLUSION

Due to the fastest growth of IoT systems, it pertains to more cyber-threat. A Botnet attack is one of the challenging cyber-attacks in IoT environment. In this paper, we have proposed an NIDS using an ensemble approach based on classification techniques such as DT, NB and SVM to detect botnet attacks against HTTP and DNS protocol. Also, it proved that the proposed ensemble framework produces better results compared to each technique included in the framework. An IoT environment architecture proposed with fog nodes, where NIDS placed. Thus, it reduces the overhead of each node in a IoT network. In Future work, test bed must implement to test the efficiency of proposed NIDS in real time data traffic.

REFERENCES

[1] P.Kazienko and P. Dorosz, "Intrusion detection systems (IDS) Part I—(Network intrusions; attack symptoms; IDS tasks; and IDS architecture)," vol. 20, no. 2009, Apr. 2003

[2] Vivekanandam, B. "Design an Adaptive Hybrid Approach for Genetic Algorithm to Detect Effective Malware Detection in Android Division." Journal of Ubiquitous Computing and Communication Technologies 3, no. 2 (2021): 135-149.

[3] G. Giacinto and F. Roli, "An approach to the automatic design of multiple classifier systems," Pattern Recognit. Lett., vol. 22, no. 1, pp. 25–33, 2001.

[4] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," Comput. Security, vol. 24, no. 4, pp. 295–307, 2005.

[5] Dewan Md. Farid , Li Zhang ,Chowdhury Mofizur Rahman, M.A. Hossain , Rebecca Strachan," Hybrid decision tree and naïve Bayes classifiers for multi-class classification tasks", 0957-4174/$ - see front matter 2013 Elsevier Ltd. All rights reserved.http://dx.doi.org/10.1016/j.eswa.2013.08.089

[6] Yan NaungSoe ,Yaokai Feng , Paulus InsapSantosa , Rudy Hartanto and Kouichi Sakurai, "Machine Learning-Based IoT-Botnet Attack Detection with Sequential Architecture", Sensors 2020, 20,4372,doi:10.3390/s20164372

[7] Mohammad Shorfuzzaman "Detection of cyber attacks in IoT using tree-based ensemble and feedforward neural network", 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC) October 11-14, 2020. Toronto, Canada

[8] S. K. Malladi, T. M. Ravi, M. K. Reddy, and K. Raghavendra, "Edge intelligence platform, and internet of things sensor streams system," Mar. 2 2017, uS Patent App. 15/250,720. 2327-4662

[9] The-UNSW-NB15-dataset, March 2018. [Online]. Available: https: //www.unsw.adfa.edu.au/australian-centre-for-cybersecurity/ cybersecurity/ADFA-NB15-Datasets/

[10] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," in Proc. IEEE Military Commun. Inf. Syst. Conf. (MilCIS), 2015, pp. 1–6.

[11] D. M. Farid, L. Zhang, C. M. Rahman, M. A. Hossain, and R. Strachan, "Hybrid decision tree and naïve bayes classifiers for multi-class classification tasks," Expert Syst. Appl., vol. 41, no. 4, pp. 1937–1946, 2014

[12] T.-S. Wang, H.-T. Lin, W.-T. Cheng, and C.-Y. Chen, "Dbod: Clustering and detecting dga-based botnets using dns traffic analysis," Computers & Security, vol. 64, pp. 1–15, 2017.

[13] Sathesh, A. "Enhanced soft computing approaches for intrusion detection schemes in social media networks." Journal of Soft Computing Paradigm (JSCP) 1, no. 02 (2019): 69-79

[14] P. Kazienko and P. Dorosz, "Intrusion detection systems (IDS) Part I—(Network intrusions; attack symptoms; IDS tasks; and IDS architecture)," vol. 20, no. 2009, Apr. 2003 Y. Bouzida and F. Cuppens, "Neural networks vs. decision trees for intrusion detection," in Proc. IEEE/IST Workshop Monitor. Attack Detect. Mitigat. (MonAM), vol. 28, 2006, p. 29.