NSS
*Neutrosophic Sets and Systems, Vol. 87, 2025*
University of New Mexico

# Neutrosophic Set and Machine Learning Model for Identifying Botnet Attacks on IoT Effectively

Wasal S AL-Bash AL-Azzawi[1], Hassan W. Hilou[2], Nawfal H. warush[3], Hasan Meslmani[4], Ahmed A El-Douh[5,6], Ahmed Abdelhafeez[5,7]

[1]Computer Engineering Technology, Al-Salam University College, Baghdad, Iraq

[2]Computer Engineering Techniques, Al-Ma'moon University College, Baghdad, Iraq

[3]Mechanical Engineering, Al-Nahrain University, Baghdad, Iraq

[4]Medical Instrumentation Techniques Engineering Department, College of Engineering Technology, Ashur University, Baghdad Iraq

[5]Applied Science Research Center, Applied Science Private University, Amman

[6]Information Systems Department, Faculty of Information Systems and Computer Science, October 6 University, Giza, 12585, Egypt

[7]Computer Science Department, Faculty of Information Systems and Computer Science, October 6 University, Giza, 12585, Egypt

**Abstract**: Botnet attacks, in which attackers utilize reciprocal communications between IoT devices to undertake extensive harmful actions, are one of the most significant risks in WSNs. In this sense, advancements in the realm of dependable and effective defenses against this kind of threat—specifically, trustworthy techniques for detecting, recognizing, and thwarting botnet attacks—are becoming more and more significant and pertinent. This work offers a thorough analysis that successfully detects botnet assaults on the Internet of Things by using machine learning techniques, including Random Forest and LSTM. These algorithms are examined, contrasted, and demonstrated to be very successful in identifying intricate patterns suggestive of botnet activity, leading to a notable enhancement in IoT security. The goal of the study is to help solve the issue of WSN and IoT security in general. The neutrosophic set is used in this study to overcome uncertainty information. We triangular neutrosophic model to select the best model. The results show RF is the best compared to other models.

**Keywords**: Machine Learning Model; Neutrosophic Set; Botnet Attacks; IoT Attacks; Attacks Detection.

## 1. Introduction

Although there are many potentially harmful attacks that may be launched using Internet of Things (IoT) devices, IoT-based botnet assaults are the most frequent.[1], [2]. The rationale is that, in comparison to traditional computer network assaults, an IoT botnet expands more quickly and has greater repercussions.

Without the Internet of Things, which has become a necessary component of our everyday life, the modern world would be unimaginable. A part of the Internet of Things, WSN is crucial to the collection of data for the larger IoT system.[3], [4]. IoT devices provide connection, data collection, and processing automation in anything from smart homes to industrial systems. However, the number of risks to these devices' security is rising in tandem with their widespread use. Botnet assaults rank among the most severe and pervasive. IoT systems are under considerable risk from this, as it may spread quickly and have detrimental effects.[5], [6]. The complexity and dynamic nature of botnet assaults sometimes render traditional security methods ineffectual.

Because of the growing risks connected to the quick spread of IoT devices, this research is relevant. It is crucial to remember that IoT device security and privacy are essential to their proper functioning; as a result, creating efficient attack detection methods is a crucial responsibility.[7], [8]. To increase the efficacy of security measures, the primary goal of this project is to examine the use of machine learning algorithms for botnet attack detection in Internet of Things environments.[9], [10].

Neutrosophy, a school of philosophy that offers a way to mimic the potential and neutralities that refer to the gray region between the positive and the negative that is typical of most real-life situations, is the source of the Neutrosophic set (NS)[11].

This kind of problem is an illustration of an Intuitionistic Fuzzy Set (IFS) and a Fuzzy Set (FS) that an NS with indeterminacy membership may manage. As a result, the idea of NS can be helpful in solving a variety of decision-making issues involving human knowledge, which is frequently tainted by ambiguity, indeterminacy, and inconsistent information. The same issues plague fields including applied physics, topology, social science, image processing, and artificial intelligence[12].

Smarandache introduced the idea of NS based on the FS and its expanded ideas (interval valued FS, intuitionistic FS, etc.) by adding an independent indeterminacy association function to the Atanassov-proposed IFs model. In the literature, several NS extensions and special instances have been proposed. NSs have garnered a lot of interest lately and have emerged as an intriguing study topic.[13].

NSs are widely used in the fields of economics, management science, operations research, natural science, military affairs, and urban planning[14], [15]. When the ambiguity and complexity of the qualities make it hard to explain or evaluate the problems with actual numbers, they can also be used to solve decision-making challenges.[16], [17].

The main objectives of this study are:

Introduce different ML models for identifying botnet Attacks on IoT Effectively.

We use random forest with different estimators and an LSTM model for better accuracy and performance.

The triangular neutrosophic model is used to overcome uncertainty in information and select the best ML model in this study.

**2. Neutrosophic and ML Model**

This section shows the neutrosophic and ML models to rank ML models and select the best one. We use triangular neutrosophic sets (TNSs) to deal with uncertainty and vague information. TNS can be defined by[18], [19]

$$Y = \left((Y_1, Y_2, Y_3); T_Y, I_Y, F_Y\right) \tag{1}$$

$T_Y, I_Y, F_Y$ Can be defined by:

$$T_Y(Z) = \begin{cases} T_Y\left(\frac{Z-Y_1}{Y_2-Y_1}\right) & if\ Y_1 \le Z \le Y_2 \\ T_Y & if\ Z = Y_2 \\ T_Y\left(\frac{Y_3-Z}{Y_3-Y_2}\right) & if\ Y_2 \le Z \le Y_3 \\ 0 & otherwise \end{cases} \tag{2}$$

$$I_Y(Z) = \begin{cases} \frac{(Y_2-Z+I_Y(Z-Y_1))}{(Y_2-Y_1)} & if\ Y_1 \le Z \le Y_2 \\ I_Y & if\ Z = Y_2 \\ \frac{(Z-Y_2+I_Y(Y_3-Z))}{(Y_3-Y_2)} & if\ Y_2 \le Z \le Y_3 \\ 1 & otherwise \end{cases} \tag{3}$$

$$F_Y(Z) = \begin{cases} \frac{(Y_2-Z+F_Y(Z-Y_1))}{(Y_2-Y_1)} & if\ Y_1 \le Z \le Y_2 \\ F_Y & if\ Z = Y_2 \\ \frac{(Z-Y_2+F_Y(Y_3-Z))}{(Y_3-Y_2)} & if\ Y_2 \le Z \le Y_3 \\ 1 & otherwise \end{cases} \tag{4}$$

Let $Y = \left((Y_1, Y_2, Y_3); T_Y, I_Y, F_Y\right)\ and\ R = \left((R_1, R_2, R_3); T_R, I_R, F_R\right)$ Two triangular neutrosophic numbers (TNNs) and their operations can be defined by:

$$Y + R = \left((Y_1 + R_1, Y_2 + R_2, Y_3 + R_3);\ T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) \tag{5}$$

$$Y - R = \left((Y_1 - R_3, Y_2 - R_2, Y_3 - R_1);\ T_Y \wedge T_R, I_Y \wedge I_R, F_Y \wedge F_R\right) \tag{6}$$

$$Y^{-1} = \left(\left(\frac{1}{Y_3}, \frac{1}{Y_2}, \frac{1}{Y_1}\right);\ T_Y, I_Y, F_Y\right) \tag{7}$$

$$\sigma Y = \begin{cases} \left((\sigma Y_1, \sigma Y_2, \sigma Y_3);\ T_Y, I_Y, F_Y\right) & if\ \sigma > 0 \\ \left((\sigma Y_3, \sigma Y_2, \sigma Y_1);\ T_Y, I_Y, F_Y\right) & if\ \sigma < 0 \end{cases} \tag{8}$$

$$YR = \begin{cases} \left((Y_1R_1, Y_2R_2, Y_3R_3); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 > 0, R_3 > 0) \\ \left((Y_1R_3, Y_2R_2, Y_3R_1); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 < 0, R_3 > 0) \\ \left((Y_3R_3, Y_2R_2, Y_1R_1); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 < 0, R_3 < 0) \end{cases} \tag{9}$$

$$\frac{Y}{R} = \begin{cases} \left(\left(\frac{Y_1}{R_3}, \frac{Y_2}{R_2}, \frac{Y_3}{R_1}\right); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 > 0, R_3 > 0) \\ \left(\left(\left(\frac{Y_3}{R_3}, \frac{Y_2}{R_2}, \frac{Y_1}{R_1}\right)\right); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 < 0, R_3 > 0) \\ \left(\left(\left(\frac{Y_3}{R_1}, \frac{Y_2}{R_2}, \frac{Y_3}{R_3}\right)\right); T_Y \wedge T_R, I_Y \vee I_R, F_Y \vee F_R\right) & if(Y_3 < 0, R_3 < 0) \end{cases} \tag{10}$$

To choose the best attack detection methods or approaches, all training methods were evaluated in terms of attack kinds, attack detection methodologies, and datasets. During the classification stage, several individual and ensemble classifiers, including machine learning techniques, were employed.

An attack detection system on an Internet of Things network that uses a unique hybrid strategy to cut down on characteristics is described in the study. In the paper's binary and multilevel classification tasks, random forest (RF) routinely performs better in terms of accuracy than other models when compared to other machine learning techniques. This implies that a key method for achieving high accuracy in identifying threats in IoT networks is machine learning. Furthermore, the model's performance is significantly impacted by the dataset selection[20], [21].

In IoT systems, machine learning techniques are useful instruments for identifying botnet attacks. Organizations can enhance the security of IoT devices and networks thanks to their capacity to analyze vast volumes of data and identify subtle trends.

## 3. Results and Discussion

This section shows the results of ML models. The outcomes of multiclass categorization of botnet assaults with dataset detection using Random Forest machine learning methods are displayed in this section. To detect Mirai and Bashlite attacks, this study makes use of the N-BaIoT dataset, which was gathered from actual network traffic of IoT devices, including both benign and attack activity. Figure 1 shows the distribution of different classes in the dataset. Figure 2 shows the rate of each class.

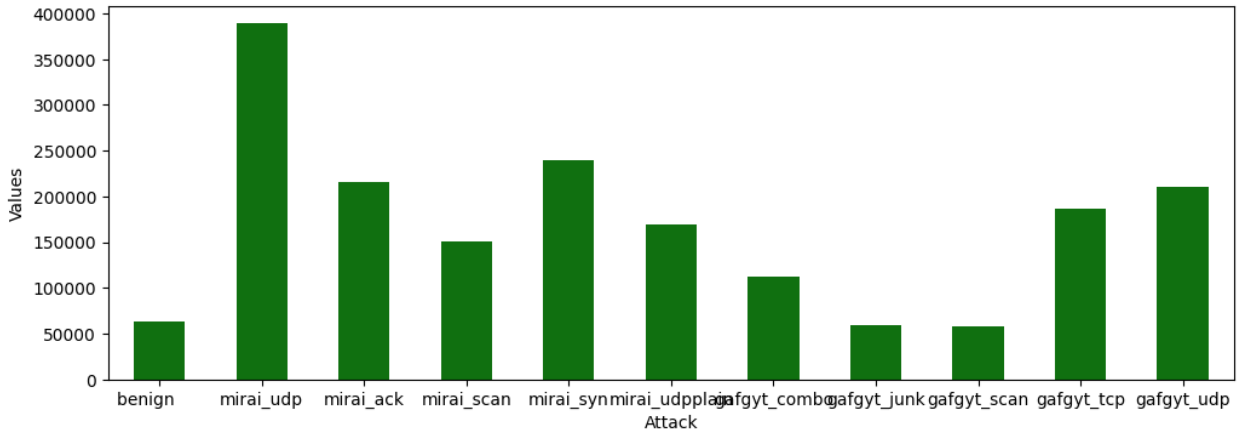


Figure 1. Distribution of classes.

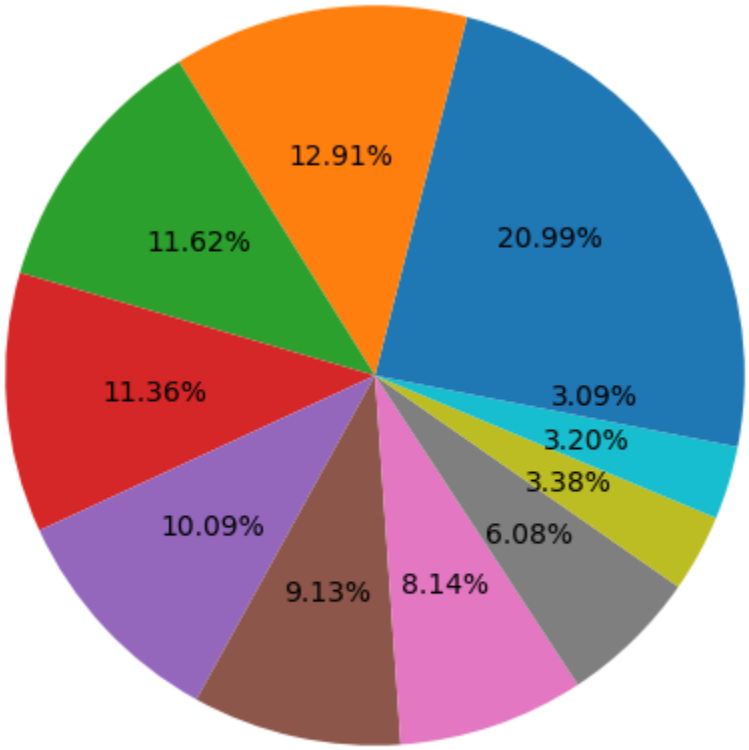


Figure 2. Rate of each class.

We use Standard Scaler to normalize the dataset. We divided the dataset into 70% for training and 30% for testing. We use four evaluation matrices to evaluate the ML models, such as accuracy, precision, recall, and F1-score. Table 1. Shows the evaluation matrices' results.

Table 1. Results of ML models.

| | Accuracy | Precision | Recall | F1-score |
|---|---|---|---|---|
| LSTM | 0.9421 | 0.949 | 0.9421 | 0.9219 |
| RF by 10 estimators | 0.942669 | 0.962278 | 0.942669 | 0.922492 |
| RF by 40 estimators | 0.942665 | 0.962275 | 0.942665 | 0.922487 |
| RF by 100 estimators | 0.939705 | 0.962692 | 0.939705 | 0.91957 |
| RF by 50 estimators | 0.942669 | 0.962281 | 0.942669 | 0.922492 |
| RF by 20 estimators | 0.942665 | 0.961902 | 0.942665 | 0.922482 |
| RF by 30 estimators | 0.942669 | 0.962279 | 0.942669 | 0.922492 |

Then we show the steps of the neutrosophic models to rank ML models. Three experts use triangular neutrosophic numbers to evaluate the ML models as shown in Table 2. Then these numbers are combined and computed the criteria weights using the average method as 0.17480719, 0.340073166, 0.227358117, 0.257761519.

Table 2. Triangular Neutrosophic Numbers.

| | $BOTC_1$ | $BOTC_2$ | $BOTC_3$ | $BOTC_4$ |
|---|---|---|---|---|
| LSTM | ((1,1,1);0.5,0.5,0.5) | ((2,3,4);0.3,0.75,0.70) | ((4,5,6);0.8,0.15,0.20) | ((6,7,8);0.9,0.10,0.10) |
| RF by 10 estimators | ((6,7,8);0.9,0.10,0.10) | ((9,9,9);1.00,0.00,0.00) | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) |
| RF by 40 estimators | ((4,5,6);0.8,0.15,0.20) | ((3,4,5);0.35,0.60,0.40) | ((3,4,5);0.35,0.60,0.40) | ((1,2,3);0.4,0.60,0.65) |
| RF by 100 estimators | ((2,3,4);0.3,0.75,0.70) | ((1,2,3);0.4,0.60,0.65) | ((1,1,1);0.5,0.5,0.5) | ((3,4,5);0.35,0.60,0.40) |
| RF by 50 estimators | ((1,1,1);0.5,0.5,0.5) | ((9,9,9);1.00,0.00,0.00) | ((2,3,4);0.3,0.75,0.70) | ((1,1,1);0.5,0.5,0.5) |
| RF by 20 estimators | ((3,4,5);0.35,0.60,0.40) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) | ((2,3,4);0.3,0.75,0.70) |
| RF by 30 estimators | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) |
| | $BOTC_1$ | $BOTC_2$ | $BOTC_3$ | $BOTC_4$ |
| LSTM | ((6,7,8);0.9,0.10,0.10) | ((2,3,4);0.3,0.75,0.70) | ((4,5,6);0.8,0.15,0.20) | ((6,7,8);0.9,0.10,0.10) |
| RF by 10 estimators | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) |
| RF by 40 estimators | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((1,2,3);0.4,0.60,0.65) |
| RF by 100 estimators | ((2,3,4);0.3,0.75,0.70) | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) |
| RF by 50 estimators | ((1,1,1);0.5,0.5,0.5) | ((9,9,9);1.00,0.00,0.00) | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) |
| RF by 20 estimators | ((3,4,5);0.35,0.60,0.40) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) | ((1,2,3);0.4,0.60,0.65) |
| RF by 30 estimators | ((1,2,3);0.4,0.60,0.65) | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) |
| | $BOTC_1$ | $BOTC_2$ | $BOTC_3$ | $BOTC_4$ |
| LSTM | ((2,3,4);0.3,0.75,0.70) | ((2,3,4);0.3,0.75,0.70) | ((4,5,6);0.8,0.15,0.20) | ((2,3,4);0.3,0.75,0.70) |
| RF by 10 estimators | ((9,9,9);1.00,0.00,0.00) | ((9,9,9);1.00,0.00,0.00) | ((2,3,4);0.3,0.75,0.70) | ((9,9,9);1.00,0.00,0.00) |
| RF by 40 estimators | ((3,4,5);0.35,0.60,0.40) | ((3,4,5);0.35,0.60,0.40) | ((9,9,9);1.00,0.00,0.00) | ((3,4,5);0.35,0.60,0.40) |
| RF by 100 estimators | ((2,3,4);0.3,0.75,0.70) | ((1,2,3);0.4,0.60,0.65) | ((3,4,5);0.35,0.60,0.40) | ((2,3,4);0.3,0.75,0.70) |
| RF by 50 estimators | ((2,3,4);0.3,0.75,0.70) | ((9,9,9);1.00,0.00,0.00) | ((2,3,4);0.3,0.75,0.70) | ((9,9,9);1.00,0.00,0.00) |
| RF by 20 estimators | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) | ((3,4,5);0.35,0.60,0.40) |

| | | | | |
|---|---|---|---|---|
| RF by 30 estimators | ((3,4,5);0.35,0.60,0.40) | ((9,9,9);1.00,0.00,0.00) | ((6,7,8);0.9,0.10,0.10) | ((4,5,6);0.8,0.15,0.20) |

The criteria weights are multiplied by the decision matrix as shown in Table 3. Then the sum of each row is computed as shown in Figure 3. The rank of ML models is obtained in Figure 3.

Table 3. The weighted decision matrix.

| | $BOTC_1$ | $BOTC_2$ | $BOTC_3$ | $BOTC_4$ |
|---|---|---|---|---|
| LSTM | 0.501478 | 0.325195 | 1.044426 | 1.300085 |
| RF by 10 estimators | 1.592931 | 3.098917 | 0.203201 | 2.609835 |
| RF by 40 estimators | 0.435925 | 1.606846 | 1.457934 | 0.322202 |
| RF by 100 estimators | 0.167159 | 0.293313 | 0.96343 | 0.865112 |
| RF by 50 estimators | 0.121272 | 3.443241 | 0.210306 | 1.788221 |
| RF by 20 estimators | 0.825964 | 2.410269 | 1.044426 | 0.330257 |
| RF by 30 estimators | 0.218509 | 3.443241 | 1.611401 | 1.184092 |

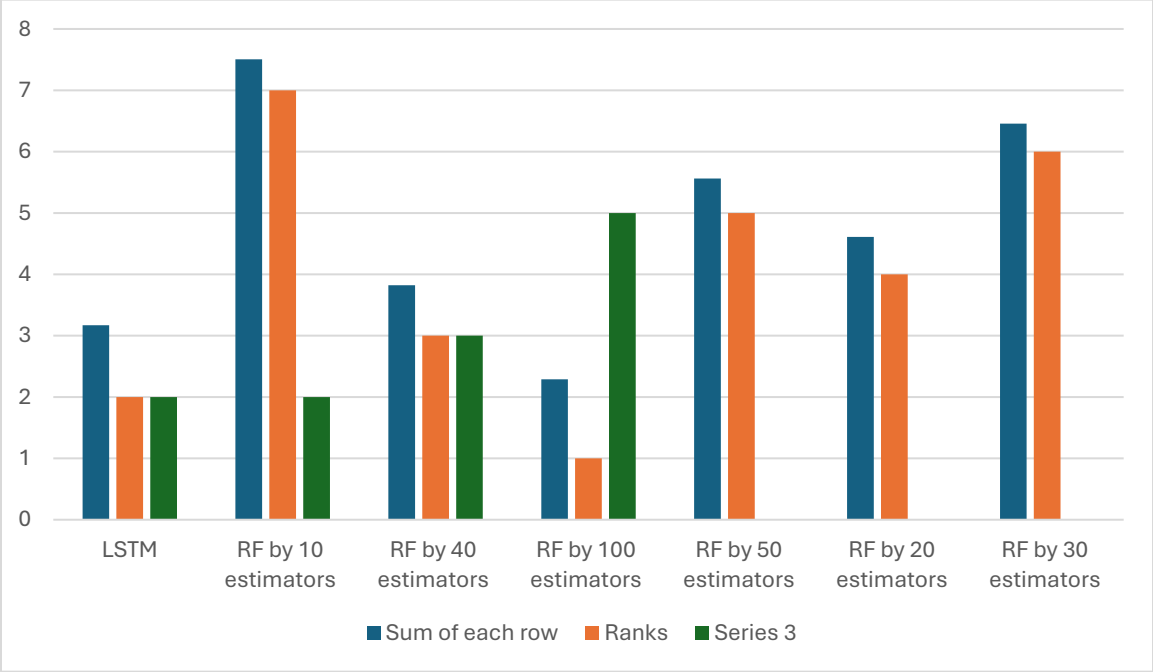


Figure 3. Rank of ML models.

The results show that RF by 10 estimators is the best ML model, and LSTM is the worst model in attack detection.

## 5. Conclusions

To sum up, this work makes a substantial addition to the field of Internet of Things security. Tested on the N-BaIoT dataset, the suggested Random Forest models demonstrated strong performance in the classification and attack detection tasks, with higher respective accuracy rates. These findings highlight how these models may be used in practical settings, particularly in

relation to Internet of Things applications. It may be inferred from the findings that the suggested Random Forest models perform similarly well. This suggests that both approaches are successful in resolving the issues of categorizing and identifying IoT device threats.

The triangular neutrosophic set is used in this study to select the best ML model. Four evaluation matrices are used in this study. The results show that RF by 10 estimators is the best ML model, and LSTM is the worst model in attack detection.

**References**

[1] S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, and E. A. Domfeh, "Ensemble machine learning techniques for accurate and efficient detection of botnet attacks in connected computers," *Eng*, vol. 4, no. 1, pp. 650–664, 2023.

[2] S. Pokhrel, R. Abbas, and B. Aryal, "IoT security: botnet detection in IoT using machine learning," *arXiv Prepr. arXiv2104.02231*, 2021.

[3] M. Injadat, A. Moubayed, and A. Shami, "Detecting botnet attacks in IoT environments: An optimized machine learning approach," in *2020 32nd International Conference on Microelectronics (ICM)*, IEEE, 2020, pp. 1–4.

[4] Z. Alothman, M. Alkasassbeh, and S. Al-Haj Baddar, "An efficient approach to detect IoT botnet attacks using machine learning," *J. High Speed Networks*, vol. 26, no. 3, pp. 241–254, 2020.

[5] M. Panda, A. M. Abd Allah, and A. E. Hassanien, "Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks," *IEEE Access*, vol. 9, pp. 91038–91052, 2021.

[6] D. Nookala Venu, A. Kumar, and M. A. S. Rao, "Botnet attacks detection in internet of things using machine learning," *NeuroQuantology*, vol. 20, no. 4, pp. 743–754, 2022.

[7] F. Hussain *et al.*, "A two-fold machine learning approach to prevent and detect IoT botnet attacks," *Ieee Access*, vol. 9, pp. 163412–163430, 2021.

[8] F. Taher, M. Abdel-Salam, M. Elhoseny, and I. M. El-Hasnony, "Reliable machine learning model for IIoT botnet detection," *IEEE Access*, vol. 11, pp. 49319–49336, 2023.

[9] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Futur. Gener. Comput. Syst.*, vol. 107, pp. 433–442, 2020.

[10] M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran, and I. Ashraf, "Hybrid machine learning model for efficient botnet attack detection in iot environment," *IEEE Access*, 2024.

[11] F. Smarandache, "Introduction to Neutrosophy, Neutrosophic Set, Neutrosophic Probability, Neutrosophic Statistics and Their Applications to Decision Making," in *Neutrosophic Paradigms: Advancements in Decision Making and Statistical Analysis:*

*Neutrosophic Principles for Handling Uncertainty*, Springer, 2025, pp. 3–21.

[12] F. Smarandache, "Foundation of superhyperstructure & neutrosophic superhyperstructure," *Neutrosophic Sets Syst.*, vol. 63, pp. 367–381, 2024.

[13] F. Smarandache, A. Saranya, A. Kalavathi, and S. Krishnaprakash, "Neutrosophic superhypersoft sets," *Neutrosophic Sets Syst.*, vol. 77, pp. 41–53, 2025.

[14] T. Fujita, "Note for neutrosophic incidence and threshold graph," *SciNexuses*, vol. 1, pp. 97–125, 2024.

[15] T. Fujita and F. Smarandache, "Pythagorean, Fermatean, and Complex Turiyam Neutrosophic Graphs," *SciNexuses*, vol. 2, pp. 39–63, 2025.

[16] F. Smarandache, P. Gayathri, E. Karuppusamy, S. Krishnaprakash, and S. Gomathi, "Optimizing Electric Vehicle Selection Using Neutrosophic SuperHyperSoft Set Theory," *Neutrosophic Sets Syst.*, vol. 86, pp. 710–729, 2025.

[17] F. Smarandache, A. M. Ali, and A. Abdelhafeez, *Single Valued Neutrosophic HyperSoft Set based on VIKOR Method for 5G Architecture Selection*. Infinite Study, 2024.

[18] E. Mathivadhana, "Modified Non-Linear Triangular Neutrosophic Numbers: Theory and Applications in Integral Equation," *Neutrosophic Sets Syst.*, vol. 72, no. 1, p. 20, 2024.

[19] Y. Liang, "Landscape Design Quality Evaluation of Abandoned Coal Mine Sites Using Single-Valued Triangular Neutrosophic Numbers," *Neutrosophic Sets Syst.*, vol. 81, no. 1, p. 26, 2025.

[20] A. H. Abed and M. A. Ebrahim, "Blood Cancer Detection from Blood Smear Images using Machine Learning Algorithms," *SciNexuses*, vol. 1, pp. 160–173, 2024.

[21] R. Karim and M. I. Asjad, "Improving Equity in Healthcare: Machine Learning-Based Thyroid Disease Classification," *SciNexuses*, vol. 1, pp. 139–147, 2024.

Received: Dec. 12, 2024. Accepted: June 23, 2025