Machine Learning Based Model for Detecting IOT-BOTNET Cyber Attacks

[1]Miss. Thorat Preeti.D, [2]Miss. Shinde Manjusha. M, [3]Miss. Tupake Pallavi. S, [4]Miss. Vaidya Pratiksha. A, [5]Prof. Patil.P.A

[1,2,3,4]UG Students, [5]Assistant Professor
Department of Computer Engineering
SND COE and RC, Yeola

***Abstract*: Due to the general expanding use of Internet of Things (IoT) systems and smart technological tools, they have now become targets for network attacks. Botnets are pre-configured attack vectors that allow attackers to take control of IoT systems and carry out malicious operations. To meet this problem, effective machine learning is required.as well as deep learning with the appropriate features to detect and protect the network from such threats, engineering is suggested.in the future, weaknesses. The representative dataset must be used to detect cyber-attacks effectively. In rare situations, the device's functionality may be delayed. To design an appropriate security model for detecting cyber threats, the representative dataset must be well-structured for training the model and then validating the proposed system in order to develop the best security possible system model**
Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

***Keywords*: Machine Learning, IOT-Botnet, Support Vector Machine, Pre- processing, Feature Extraction, Classification.**

INTRODUCTION

Because today's firewalls are unable to detect and block such a contemporary cyber security assault scenario, network attacks or intrusions are collections of events conveyed by network packets that pose a threat to the confidentiality, availability, and integrity of the IoT network. Furthermore, with the widespread use of smart digital devices in an IoT network environment, secure communications among such interconnected devices is becoming increasingly important as the network grows. Getting vulnerabilities out of an IoT network system is difficult and expensive. It has recently been shown that an effective network intrusion detection system can not only detect modern security threats, including zero-day attacks, but also prevent them from happening in the future

MOTIVATION

1. In recent, Digital Communication increases rapidly.

2. It is difficult to maintain cyber security and detecting cyber treats

LITRATURE SURVEY

ARBA: Anomaly and Reputation Based Approach for Detecting Infected IoT Devices: An Anomaly Detection loT (AD-IoT) system, which is an intelligent anomaly detection based on Random Forest machine learning algorithm.

1. **HTTP Botnet Detection in IOT Devices using Network Traffic Analysis**: The results can help us know the potential of applying Machine Learning algorithms to the IoT network behavior dataset.

2. **Identification of Botnet Activity in IoT Network Traffic Using Machine Learning**: The classifiers can also separate malicious activity from benign activity in increasingly larger datasets. Our experiments have demonstrated incremental improvement in results for accuracy, probability of detection, and probability of false alarm.4. IoT DDOS ATTACK DETECTION USING MACHINE LEARNING: In this Study We build a proposed framework to detect and abnormal defense activities. Impact of IoT-specific features like insufficient processing power, power limitations, and node density.

5. **AD-IoT: Anomaly Detection of IoT Cyber-attacks Smart City Using Machine Leaming**: The IoT cyber security threats in a smart city, we propose an Anomal Detection IoT system, which is detection based on Random Forest machine learning algorithm

LIMITATION OF EXISTING SYSTEM

- **Costing:** The Existing system is high cost and this is main reason most of the system is failed.
- **Technology Complexity:** Most of system is the complex to understand, not user friendly as compare to our proposed system
- **Time Consuming Feature:** In existing system, the performance is low and most of the time system gets hanged due to load.
- **Not Easy to Understand:** Systems re complex to understand and they were not user friendly

EXPERIMENTAL SETUP

Python:
Python is an interpreted, high-level and general-purpose programming language. Created by Guido van Rossum and first released in 1991, Python's design philosophy emphasizes code readability with its notable use of significant whitespace. Its language constructs and object oriented approach aim to help programmers write clear, logical code for small and large-scale projects.
Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured (particularly, procedural), object-oriented, and functional programming. Python is often described as a "batteries included" language due to its comprehensive standard library.
Python was created in the late 1980s as a successor to the ABC language. Python 2.0, released in 2000, introduced features like list comprehensions and a garbage collection system with reference counting.

Anaconda:
Anaconda is a free and open-source distribution of the Python and R programming languages for scientific computing (data science, machine learning applications, large-scale data processing, predictive analytics, etc.), that aims to simplify package management and deployment. The distribution includes data-science packages suitable for Windows, Linux, and macOS. It is developed and maintained by Anaconda, Inc., which was founded by Peter Wang and Travis Oliphant in 2012. As an Anaconda, Inc. product, it is also known as Anaconda Distribution or Anaconda Individual Edition, while other products from the company are Anaconda Team Edition and Anaconda Enterprise Edition, both of which are not free.
Package versions in Anaconda are managed by the package management system conda. This package manager was spun out as a separate open-source package as it ended up being useful on its own and for other things than Python. There is also a small, bootstrap version of Anaconda called Miniconda, which includes only conda, Python, the packages they depend on, and a small number of other packages.

SCOPE:
Various malwares are exploiting the vulnerabilities in IoT devices, resulting in large scale Cyber - attacks. In this propose system, we propose a novel approach for detecting IoT-botnet cyber-attacks. Based on botnet behavior analysis. We use supervised machine learning techniques with the observed attributes as inputs to detect the presence of these botnet cyber
Attacks. We also used a variety of different machine-learning techniques and find its suitability for efficient detection of IoT botnet cyber-attacks.

PROBLEM STATEMENT:
In current digital era, cyber security is critical to maintain a high degree of safety due to the increasing use of digital communication. This form of assault is difficult to detect because the device continues to function normally, and the user or owner of the device will not realize whether his gadget is a victim of an attack. In rare situations, the device's functionality may be delayed. To design an appropriate security model for detecting cyber threats, the representative dataset must be well-structured for training the model and subsequently testing the proposed system.

SYSTEM ARCHITECTURE:

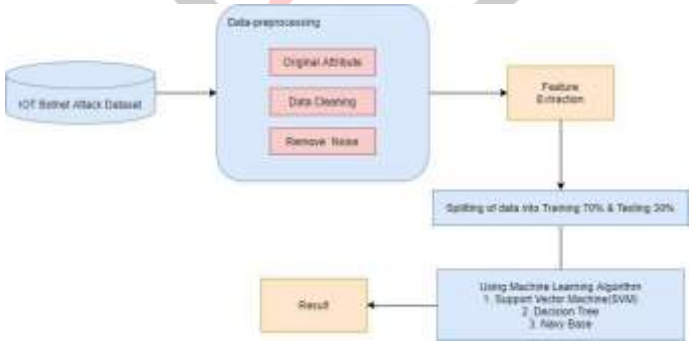


Fig-1: System Architecture Diagram

The major requirement for implementing this project using python programming language along with the machine learning. Computer vision and also python libraries. It can be use high and low computation scenarios. We are using SVM, Navy Base, and Decision tree in our proposed system.

MATHEMATICAL MODEL

Let S be the Whole system S= I,P,O I-input

P-procedure O-output Input (I)

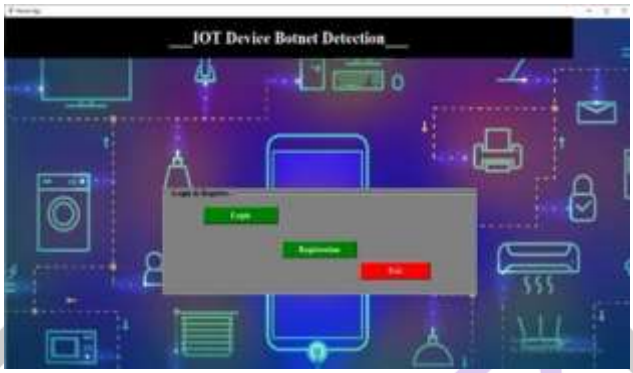
I= Botnet Dataset Where,

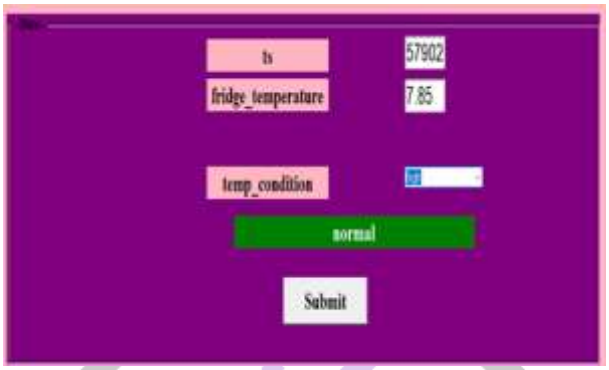
Dataset contain botnet as textual Format Procedure (P),

P=I, Using I System perform operations and calculate the prediction

1. Pre-processing.
2. Feature Extraction.
3. Classification (Apply Different ML Algorithm).

Screenshots:





ADVANTAGES:

a. It is User-friendly System.
b. Easy find efficient detection of IoT-botnet cyber- attacks.
c. Improve Best Accuracy.

APPLICATION:

- System can be implemented where mostly IOT devices are used.
- System can be used by every person for protecting there IOT devices from various attacks.
- System provides higher accuracy to detect BOTNET attacks.
- System can be used by any organization for keeping IOT devices secure from BOTNET attacks.

METHODOLOGY

The line that maximizes the minimum margin is a good bet. The model class of "hyper-planes with a margin of m" has a low VC dimension if m is big. This maximum-margin separator is determined by a subset of the data points. Data points in this subset are called "support vectors" .It will be useful computationally if only a small fraction of the data points are support vectors, because we use the support vectors to decide which side of the separator a test case is on.

1. **P Class**: • P is set of all decision problems which can be solved in polynomial time by a deterministic.
- Since it can be solved in polynomial time, it can be verified in polynomial time.
- Therefore P is a subset of NP. P: to detect cyber-attacks.

2. **NP Class**: NP means we can solve it in polynomial time if we can break the normal rules of step-by-step computing.

(a) NP Hard Problems: A problem is NP-hard if an algorithm for solving it can be translated into one for solving any NP-problem (nondeterministic polynomial time) problem. NP-hard therefore means "at least as hard as any NP-problem," although it might.

(b) NP complete problems: We have used machine learning algorithms to detect IOT botnet cyber-attacks. Hence the 'P' is NP-Complete in this case.

CONCLUSION:

Various malwares are exploiting the vulnerabilities in IoT devices, resulting in large scale Cyber - attacks. In this propose system, we propose a novel approach for detecting IoT-botnet cyber-attacks. Based on botnet behavior analysis. We use supervised machine learning techniques with the observed attributes as inputs to detect the presence of these botnet cyber-attacks. We also used a variety of different machine-learning techniques and find its suitability for efficient detection of IoT botnet cyber-attacks.

REFERENCES

1. J. Howell. Number of connected IoT devices will surge to 125 billion by 2030, IHS markit says - IHS technology. [Online]. Available: https://technology.ihs.com/596542/, last accessed: 11/07/2018.
2. E. Borgia,"The internet of things vision: Key features, applications and open issues," Computer Communications, vol. 54, pp. 1-31, 2014.
3. F. Restuccia, S. D'Oro, and T. Melodia, "Securing the internet of things: New perspectives and research challenges," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 1-14, 2018.
4. J. A. Stankovic, "Research directions for the internet of things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.
5. M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran. Durumeric, J.A.Halderman, L.Invernizzi, M.Kallitsisetal.,"Understandingthemirai botnet;' in USENIX Security Symposium, 2017, pp. 1092- 1110.