EasyChair Preprint

№ 9187

Machine Learning-Based Mechanism for Mitigating DDOS Attacks from Smart Home IoT Networks

Izzadeen Alfaqih and Mohammed Ibrahim

October 29, 2022

Machine Learning-Based Mechanism for Mitigating DDOS Attacks from Smart Home IoT Networks

Izzadeen Abdulaziz Alfaqih, CGS,Taiz University,Yemen
Email: Izzadeen.Alfaqih@yahoo.com
Prof. Dr Mohammed A.M.Ibrahim, Faculty of Engineering ,Taiz University,Yemen
Email: sabri1966@yahoo.com

ABSTRACT

In recent decades, Internet of things (IoT) has increasingly become a ubiquitous widespread intelligent technology worldwide. It provides different advanced applications such as business, health, communications, smart home, industry, smart cities, and agriculture. the IoT is considered the main target for internet pirates and hackers looking for sensitive information or/and exploit it to destroy service provider's networks. Most recently, a denial of service (DoS) or distributed denial of service (DDoS) attack is the most common security concern allows attackers to make online systems unavailable to legitimate users. This paper aim to investigate the current architecture and mechanism used in IoT, also we propose a novel DDoS detection and mitigation cybersecurity model by using Machine learning (ML) approach through a set of modern IoT datasets. Finally, it could evaluate the develop model in term of security evolution metrics and could shed light on some future research directions that need further investigation.

Key words: Internet of things (IoT), denial of service (DoS), distributed denial of service (DDoS), and Machine learning (ML).

1. INTRODUCTION

With the rapid and tremendous progress in the current era, technology has become a necessity in all aspects of human daily life. Therefore, this has led to the emergence and growth of Internet of Things (IoT) objects which will lead to an improvement in the quality of life [1]. In 1999, a new intelligent technology term which called IoT (Internet of Things) is invented by Kevin Ashton, which refers to the things connected to the Internet to collect and share data in order to reach the planned goals [2], and it consists of four main components: objects, applications, communication, and data analysis [3]. These things such as sensor, smart TV, smart watches, smart bicycle, smart refrigerators, smart door lock and others. IoT becomes the cornerstone of many applications especially in 4.0 industrial revolution technologies and communications, Figure [1.1] represents the 4.0 industry framework-digital technologies [4]. Moreover, IoT contributes to many fields such as agriculture, environment, medical sector, education, transportation, economic and others.

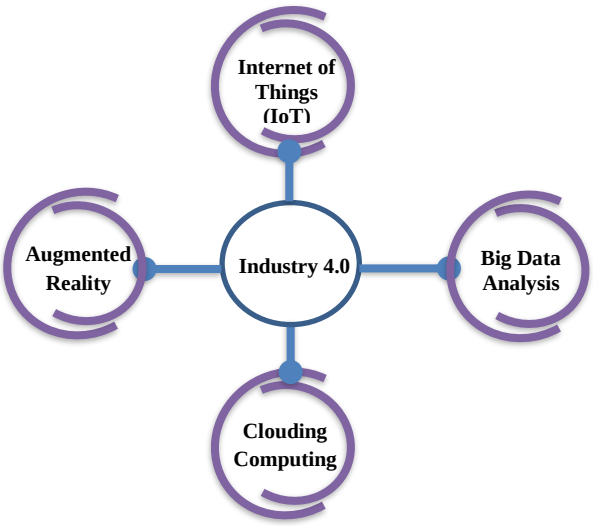

Figure [1. 1]: Industry 4.0 Framework

1.1 IoT Statistics:

IoT has become an integral part of our daily lives and is widely spread in various areas of life. According to precedents, Figure [1.2] illustrates a statistic on the expected number (in billions) of Internet of Things (IoT) devices to be connected worldwide between 2019 and 2030 [5], where it has expected that the IoT will reach in 2022 about 11.57 billion, in 2023 about 13.15 billion, and in 2030 about 25.44,which means approximately 20% annual increase.

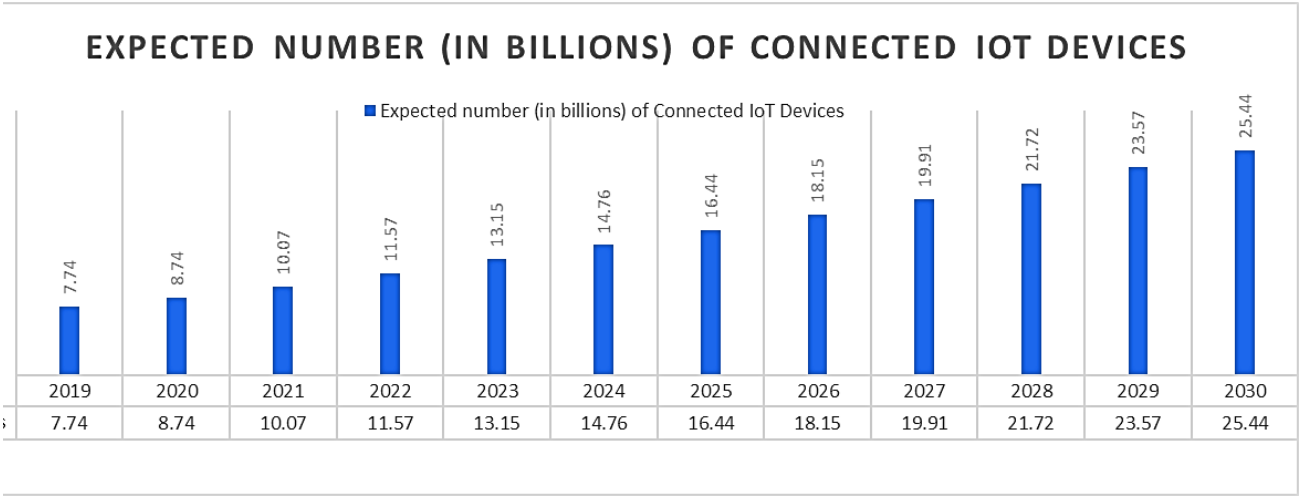

Figure [1. 2]: Statistic on the expected number (in billions) of IoT devices (2019 to 2030)

1.2 IoT Layers Architectures:

In Fact, one of the main challenges that any technology face is to develop a reference architecture. There is no a single general architecture for IoT [6], because of variety and difference in IoT applications, the following shows most of the IoT architectures.

A 3-layer Architecture is the main diagram of the Internet of Things [7] and it consists of the perception layer, network layer, and application layer as shown in Figure [1.3]. The perception layer is the layer of the physical IoT objects [4], and sensors which interact with the surrounding environment. This layer is responsible for collecting information converted into digital signals, processed, and then transmitted into the network layers, while the network layer is considered as a link between the perception layer and the application layer. Finally, the application layer is a software layer that has specific services and this layer of storing, collecting, filtering and processing data. In addition, it uses different number of protocols.

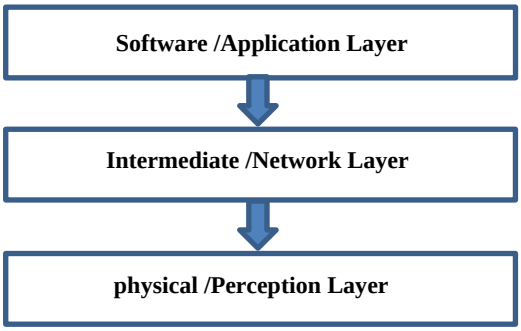

Figure [1. 3]: 3-Layer IoT Architecture

Due to the limitations of the previous architecture (3-Layer IoT Aechitecture), a new architecture consisting of four layers was proposed by adding a new layer over the previous architecture, called the support layer [8], figure [1.4] shows the five-layer structure of the Internet of Things.

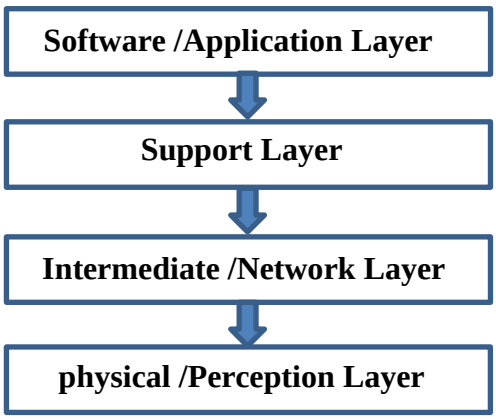

Figure [1. 4]: 4-Layer IoT Architecture

In this third type of IoT architecture, two new layers have been added, a business layer and a processing layer. The five-layer IoT architecture is also built based on the 3-Layer IoT Architecture. The figure [1.5] shows the five-layer structure of the Internet of Things [9].

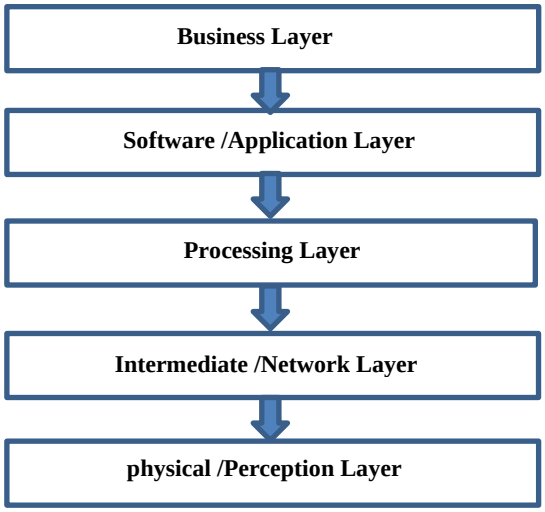

Figure [1. 5]: 5-Layer IoT Architecture

1.3 IoT Challenges:

Cybersecurity in IoT is an essential topic exposed to the risks of cyber-attacks. Alongside, IoT devices are not homogeneous because they are made by different manufacturers, which leads to the difficulty of providing a consistent level of protection and security for these devices. Therefore, other approaches must be designed to protect against IoT vulnerable devices. this research seeks to develop Machine Learning-Based DDoS cybersecurity model to improve the security from vulnerable IoT attacks

1.4 IoT Security Threats:

IoT system has a number of serious drawbacks, heterogeneity and complexity are the most significant problem because IoT operations are very complex and there is no flexible integration among devices [4]. Besides, the IoT has become the main target for internet pirates and hackers looking for sensitive information., and make online systems out of service to legitimate users by sending massive DoS or DDoS attacks.

2. PAPER ORGANIZATION

Paper is prepared as follows:
Section 3 Machine Learning, section 4 Problem Statement, section 5 paper Aim and Objectives, section 6 Proposal, section 7 paper Methodology, section 8 Conclusion and future work, finally section 9 references.

3. MACHINE LEARNING:

Machine learning is one of the most popular artificial intelligence sciences in analyzing and building robust algorithms. Machine learning is divided into three main sections: supervised learning and unsupervised learning and reinforcement [10]. Each section has its own usages and algorithms. Figure shows the most general branches of machine learning.

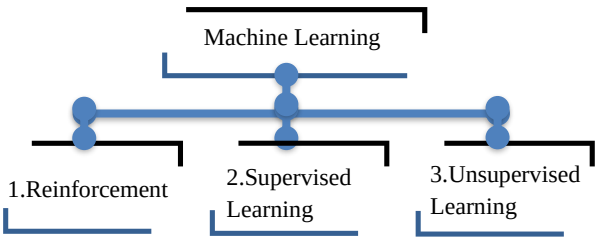

Figure [1. 6]: The Most General Branches of Machine Learning

Supervised learning is one of the most popular machine learning methodologies that relies on input-output data to perform the classification and analysis process. On the other hand, unsupervised learning depends on input data without output data for the sake of analysis and classification. However the third type (reinforcement) is concerned with interacting with the surrounding environment as humans and take actions that improve general reactions [11]. Recently, the field of machine learning has become used to develop solutions for information security, especially in the field of the Internet of Things and this field has attracted many researchers due to its important contributions to find proper solutions. Consequently, in this research, machine-learning novel model will be used to find a solution to the most important global problems (DDoS attacks) to meets the purpose of protection and security.

4. PROBLEM STATEMENT

Most recently, a denial of service (DoS) and distributed denial of service (DDoS) attack are the most popular security because the Internet of Things (IoT) includes all the smart devices surrounding on the Internet and reveals many vulnerabilities at various levels. These attacks concern that allows attackers to make online systems unavailable to legitimate users by exploit it sending a large number of packets to the target system. Besides, they are increasing the massive cost losses reaching to millions and millions of dollars annually [12]. Therefore, it has become Significantly to resist and take defenses seriously to secure IoT services, so it is necessarily need to develop cybersecurity model to address these security issues. Consequently, the main objective of this research is to contribute to develop an effective model secure the systems from DDoS attack executed by smart home IoT devices. Moreover, a machine learning technology will be used to detect, prevent, and suggest an alternative solution whenever an issue is about to occur or an unsafe state is about to happen, in terms of keeping the management aware of the current situation, which leads to understand the best next actions to be taken and to follow the best ways to ensure high level of security.

5. PAPER AIM AND OBJECTIVES

The aim of this paper is to develop DDoS cybersecurity model for improving the security in systems agonist the vulnerable IoT devices. For this aim, the objectives are as follows:

1. To investigate the current security architecture, requirements and mechanism used in Internet of Things.
2. To propose a novel DDoS detection and mitigation cybersecurity model for IoT domain.
3. To evaluate the developed model in resistance to DDoS executed by smart home IoT devices.

6. PROPOSAL OF PAPER

The science of artificial intelligence has become the most effective approach which support all other sciences, including data security by inspecting and detecting the transmitted data payload. Therefore, this paper proposes the use of machine learning in order to solve the problem of DDoS and DoS attacks through a variety of datasets. As a result of the heterogeneity problem in the structure and operation of IoT devices, it suggests that a set of data sets of different and modern IoT devices can be used. In order to reach a high-performance model, the paper proposes that data preparation can be done, for example, data cleaning, normalization and

features selection, in addition to checking the model can be conducted to test the proposed and depicting the results in clear graphs.

7. PAPER METHODOLOGY

For the success of any research, a clear methodology must be chosen with sequential robust steps. Figure [1.1] illustrates the process steps of the paper.

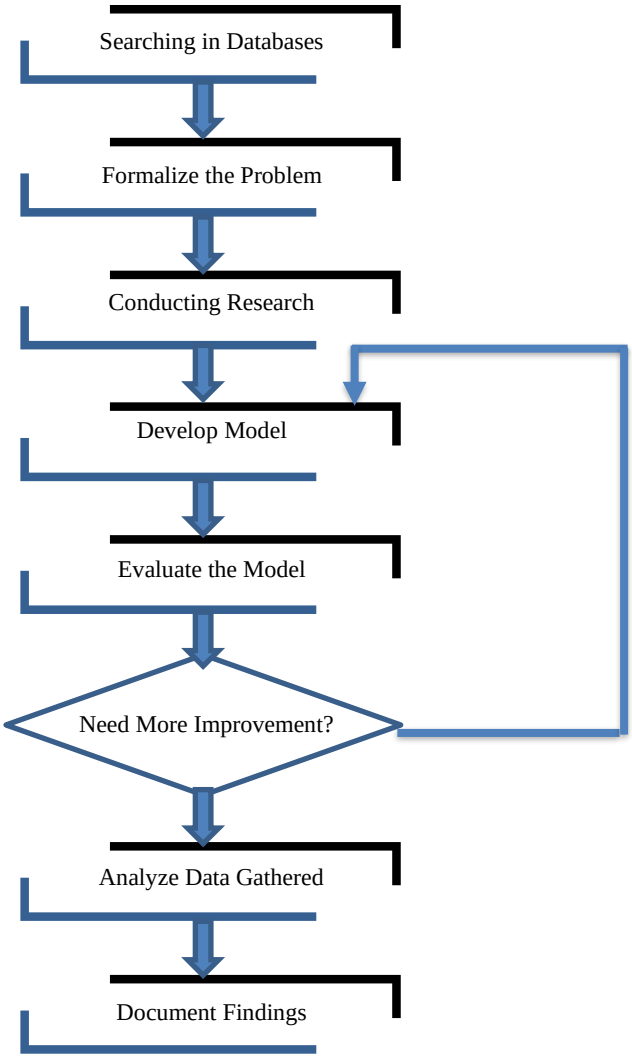

Figure [1. 7]: Research Methodology

8. CONCLUSION AND FUTURE WORK

With the wide and tremendous spread of Internet of Things applications, IoT has become in all aspects of daily life, which in turn lead to the increase in botnet attacks, so this Proposal focuses and aims to provide a new model based on machine learning in order to discover botnet attacks comes from smart home IoT networks, particularly DoS and DDoS attacks. Moreover, their role in bringing down the systems for authorized users and causing huge financial losses, whether for government, or private sectors and even individuals. A set of questions related to IoT cybersecurity has been considered in order to verify the efficacy of this proposed model. It is necessary to choose the best machine learning algorithms with the highest performance and efficiency, and to use a set of the latest datasets for training these algorithms in order to obtain a strong, robust and reliable model for detecting botnet IoT attacks. In future work, other research can be extended into diverse directions by applying this model in a real network environment, extending the application of this model to different types of attacks, and we are using deep learning algorithms instead of machine learning.

9. REFERENCES

[1] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," Proc. - 2020 Work. Emerg. Technol. Secur. IoT, ETSecIoT 2020, pp. 22–29, 2020, doi: 10.1109/ETSecIoT50046.2020.00009.

[2] A. Boukerche and R. W. L. Coutinho, "Design Guidelines for Machine Learning-based Cybersecurity in Internet of Things," IEEE Netw., vol. 35, no. 1, pp. 393–399, 2021, doi: 10.1109/MNET.011.2000396.

[3] O. I. Abiodun, E. O. Abiodun, M. Alawida, R. S. Alkhawaldeh, and H. Arshad, A Review on the Security of the Internet of Things: Challenges and Solutions, no. 0123456789. Springer US, 2021. doi: 10.1007/s11277-021-08348-9.

[4] S. O. M. Kamel and N. H. Hegazi, "A Proposed Model of IoT Security Management System Based on A study of Internet of Things (IoT) Security," Int. J. Sci. Eng. Res., vol. 9, no. 9, pp. 1227–1244, 2018, [Online]. Available: https://www.researchgate.net/profile/Samah_Kamel3/publication/328163339_A_Proposed_Model_of_IoT_Security_Management_System_Based_on_A_study_of_Internet_of_Things_IoT_Security/links/5bbc74254585159e8d8f245a/A-Proposed-Model-of-IoT-Security-Management-Syste

[5] "• IoT connected devices worldwide 2019-2030 | Statista." https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (accessed Dec. 18, 2021).

[6] M. Lombardi, F. Pascale, and D. Santaniello, "Internet of things: A general overview between architectures, protocols and applications," Inf., vol. 12, no. 2, pp. 1–21, 2021, doi: 10.3390/info12020087.

[7] M. Burhan, R. A. Rehman, B. Khan, and B. S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," Sensors (Switzerland), vol. 18, no. 9, pp. 1–37, 2018, doi: 10.3390/s18092796.

[8] D. G. Darwish and E. Square, "Improved Layered Architecture for Internet of Things," Int. J. Comput. Acad. Res., vol. 4, no. 4, pp. 214–223, 2015, [Online]. Available: http://www.meacse.org/ijcar

[9] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, 2017, doi:

10.1155/2017/9324035.

[10] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of Internet of Things (IoT): A survey,” J. Netw. Comput. Appl., vol. 161, 2020, doi: 10.1016/j.jnca.2020.102630.

[11] N. A. Stoian, “Machine learning for anomaly detection in iot networks : malware analysis on the iot-23 data set,” 2020.

[12] “Legal Implications of DDoS Attacks and the Internet of Things (IoT) | Data Protection Report.” https://www.dataprotectionreport.com/2016/12/legal-implications-of-ddos-attacks-and-the-internet-of-things-iot/ (accessed Dec. 17, 2021).