Journal of Advanced Research in Microelectronics and VLSI
Volume 7, Issue 1 - 2024, Pg. No. 5-9
Peer Reviewed Journal

Research Article

Basic Principles of Intruder Detection System

Priyanka Nanda[1], Jimmy Singla[2], Kapil Mehta[3]

[1]Research Scholar Department of Computer Science & Engineering, CT University, Punjab, India.
[2]Professor &HOS Department of Computer Science & Engineering, CT University, Punjab, India.
[3]Associate Professor Department of Computer Science & Engineering, CT University, Punjab, India.

I N F O

Corresponding Author:
Priyanka Nanda, Department of Computer Science & Engineering, CT University, Punjab, India.
E-mail Id:
priyankananda428@gmail.com
Orcid Id:
https://orcid.org/0009-0006-4297-8500
How to cite this article:
Nanda P, Singla J, Mehta J. Basic Principles Of Intruder Detection System. J Adv Res Microelec VLSI 2024; 7(1): 5-9.
Date of Submission: 2024-03-11
Date of Acceptance: 2024-04-13

A B S T R A C T

With the rapidly growing technology, IoT repercussion the whole world by their emerging features. But woefully, it has been fascinating to bring attention of intruder, who made IoT a target of venomous activities, such as cyber-physical attacks in DER systems. To protect IoT devices from cyber physical attacks, we propose a novel hybrid intruder detection system with edge computing. With this, we have to check the techniques that are used in Intruder Detection System (IDS) and the kind of attacks that deals with the mechanism pertaining to it. The proposed hybrid IDS is evaluated using BoT-IoT datasets which provides network traffic related to IoT and various types of attacks.

Keywords: Novel Hybrid Intruder Detection System, Edge Computing, Iot, Zigbee, Bot-Iot Datasets

Introduction

The term IoT, or Internet of Things, mention the network of interconnected devices and the automation that clear the way for communicate between devices and the cloud, as well as between the devices themselves. The IoT has been growing rapidly and make a significant influence on day-to-day life. With the large range of IoT devices to connected each other which have provocation tasks to secure IoT devices with different kind of attacks. To protect different kind of attacks, we propose Novel Hybrid Intrusion Detection System.

Novel Hybrid Intrusion Detection System

The Novel Hybrid Intrusion Detection System is one the exact and powerful misuse Intruder Detection System that count on some determined attack signature to differentiate between normal and venomous activities which are used to protect different kind of attacks based on machine learning techniques. To protect IoT devices with Novel Hybrid Intruder Detection System, we propose C5 classifier with KNN(K-Nearest Neighbors) machine learning algorithm.

Edge Computing

We propose Edge Computing because it helps in real-time data processing without latency, reduces privacy/security risks and optimizes the network resources. Edge Computing is used to store sensitive data in a local cloud to preserve the customers privacy.Edge Computing is a distributed computing system that allows to bringcomputation of data and storage too close to the source.Edge Computing is a faster computing method.Edge Computing is to improve the network technology by moving the computation of data close to the edge of the network and away from the data centers.

The main contributions of this paper are as follows:

- Development of techniques used in IDS based on Edge computing to improve the efficiency to select IoT devices that result in maximum differences of features amongst all the applications.
- Development of Hybrid Intrusion Detection System with Edge Computing for IoT devices that uses C5 classifier with KNN(K-Nearest Neighbors) machine learning algorithm to create an effective and improved

architecture for improving bandwidth, latency and increased performance with less cost.

- It can also demonstrated and analysed to measure the performance of the system which shows high accuracy and ability to detect unknown and new attacks.

Zigbee

Zigbee is an IEEE 802.15.4 based pattern for a suite of high-level message protocols used to create personal area network with small, low power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs. It is designed for small scale projects which need wireless connection. Hence zigbee is a low-power, low data rate and close immediacy wireless ad-hoc network. Zigbee devices can transmit data over long distances by passing data through a mesh network of in-between devices to reach more remote ones. It is typically based in low data rate applications that require long battery life and secure networking. It uses ad-hoc on demand distance vector(AODV) routing. Zigbee has two important components: They are zigbee device object (ZDO) and application support sub-layer(APS). ZDO is responsible for device management and security policies where APS is liable for interfacing and controlling devices, bridge between network and other layers.

Literature Review

AnsamKhraisat (2019) discussed the large number and diverse types of IoTdevices, it is a challenging task to protect the IoT infrastructure using a traditional intrusion detection system. To protect IoT devices, a novel ensemble Hybrid Intrusion Detection System (HIDS) is proposed by combining a C5 classifier and One Class Support Vector Machine classifier. HIDS combines the advantages of Signature Intrusion Detection System (SIDS) and Anomaly-based Intrusion Detection System (AIDS). The aim of this framework is to detect both the well-known intrusions and zero-day attacks with high detection accuracy and low false-alarm rates.

Shreeya_Jain (2022) discussed the IoT and learning algorithms in an area Machine Learning (ML) and Deep Learning (DL) has given new scope to cyber security. The security attacks on IoT networks are possible to detect and prevent intelligently using ML and DL techniques. ML and DL can make traditional attack detection methods efficient, reliable, and robust. The aim of this article is to develop the novel hybrid intrusion (attack) detection model using DL techniques, Convolutional neural network (CNN) and Long short-term memory (LSTM) to achieve better attack detection accuracy.

Ashish Singh (2022) discussed the Mobile Edge Computing (MEC) model attracts more users to its services due to its characteristics and rapid delivery approach. This network architecture capability enables users to access the information from the edge of the network. But, the security of this edge network architecture is a big challenge. All the MEC services are available in a shared manner and accessed by users via the Internet. Attacks like the user to root, remote login, Denial of Service (DoS), snooping, port scanning, etc., can be possible in this computing environment due to Internet-based remote service.

Doaa Mohamed & Osama Ismael (2023) discussed the scope of cyber-attacks on the internet of things has grown exponentially. So, it makes it a necessity to develop an efficient and accurate intrusion detection system that should be fast, dynamic, and scalable in an internet of things environment. On the other hand, Fog computing is a decentralized platform that extends Cloud computing to deal with the inherent issues of the Cloud computing. As well, maintaining a high level of security is critical in order to ensure secure and reliable communication between Fog nodes and internet of things devices.

Yar, H., Imran, A S., Khan, Z A., Sajjad, M., Kastrati, Z. (2021) discussed the e revolution in technologies has made homes more convenient, efficient, and even more secure. The need for advancement in smart home technology is necessary due to the scarcity of intelligent home applications that cater to several aspects of the home simultaneously, i.e., automation, security, safety, and reducing energy consumption using less bandwidth, computation, and cost. Our research work provides a solution to these problems by deploying a smart home automation system with the applications mentioned above over a resource-constrained Raspberry Pi (RPI) device. The RPI is used as a central controlling unit, which provides a cost-effective platform for interconnecting a variety of devices and various sensors in a home via the Internet. We propose a cost-effective integrated system for smart home based on IoT and Edge-Computing paradigm. The proposed system provides remote and automatic control home appliances, ensuring security and safety.

Yifei Li , Mingyang Yu , Sichen Li(2022) discussed the content evaluation and behavioural willingness of audiences towards different types of news written by human and computer through a 2 * 2 factorial experiment. The results indicate that people have a stronger behavioural willingness towards data-based news than non-data-based news generated by computer. While for news generated by human, people don't distinguish the types of news, but decide whether to read and share it based on the quality of the content. The public's inherent impression of AI technology is also shown in this study to moderate people's technical evaluation on behavioural willingness. Based on the research findings, the implications and suggestions are addressed accordingly.

M. Maheswari (2021) discussed the wireless communication and digital technology, low power, Internet-enabled, and reconfigurable wireless devices have been developed, which revolutionized day-to-day human life and the economy across the globe. These devices are realized by leveraging the features of sensing, processingthe data and nodes communications. The scale of Internet-enabled wirelessdevices has increased daily, and these devices are exposed to various cyberattacks.Since the complexity and dynamics of the attacks on the devices are computationallyhigh, intelligent, scalable and high-speed intrusion detection systems(IDS) are required. Moreover, the wireless devices are battery-driven; implementingthem would consume more energy, weakening the accuracy of detecting theattacks. Hence the design of the IDS is required, which has to establish the good trade-offs between Energy and accuracy.

Imran Hidayat, Muhammad Zulfiqar Ali (2023) discussed the networks are moving toward automation and getting more and more intelligent. With the advent of big data and cloud computing technologies, lots and lots of data are being produced on the internet. Every day, petabytes of data are produced from websites, social media sites, or the internet. As more and more data are produced, a continuous threat of network attacks is also growing. An intrusion detection system (IDS) is used to detect such types of attacks in the network. IDS inspects packet headers and data and decides whether the traffic is anomalous or normal based on the contents of the packet. In this research, ML techniques are being used for intrusion detection purposes. Feature selection is also used for efficient and optimal feature selection. The research proposes a hybrid feature selection technique composed of the Pearson correlation coefficient and random forest model. For the machine learning (ML) model, decision tree, AdaBoost and K-nearest neighbor are trained and tested on the TON_IoT dataset. The dataset is new and contains new and recent attack types and features.

Rabie A. Ramadan* and Kusum Yadav discussedto maintain the security of IoT systems, there is a need for an efficient Intrusion Detection System (IDS). IDS implements detectors that continuously monitor the network traffic. There are various IDs methods proposed in the literature for IoT security. However, the existing methods had the disadvantages in terms of detection accuracy and time overhead. To enhance the IDS detection accuracy and reduces the required time, this paper proposes a hybrid IDS system where a pre-processing phase is utilized to reduce the required time and feature selection as well as the classification is done in a separate stage. The feature selection process is done by using the Enhanced Shuffled Frog Leaping (ESFL) algorithm and the selected features are classified using Light Convolutional Neural Network with Gated Recurrent Neural Network (LCNN-GRNN) algorithm

Methods

Types of attacks

Network Intrusion Detection System

A Network Intrusion Detection System originate to assist different groups for check their cloud on-premises and hybrid, environments for dubious events that could indicate a compromise. A Network Intrusion Detection System is a computer suite which discover and report the problems occur in network security by observing system or network activities for venomous behaviour.

Host Intrusion Detection System

A Host intrusion Detection System is an intrusion detection system that checks the infrastructure of computer where it is installed to examine traffic and logging venomous behaviour. It is used to check and examine the internals of a computing system as web as network packets.

Network Node Intrusion Detection System

A Network Node Intrusion Detection System (NNIDS) is like a NIDS, but it's only request for one host at a single time, not an entire loop-back.It needed for unselective network which is used to analyse all traffic including all intended traffic.

Techniques used in Intrusion Detection System

Signature-based intrusion detection systems (HIDS)

Signature intrusion detection systems (SIDS) established on pattern matching techniques which is used to locate known attack; these are also known as Knowledge-based Detection or Misuse Detection. In SIDS, matching methods are used to find a previous intrusion. In other words, when an intrusion signature matches with the signature of a previous intrusion that already exists in the signature database, an alarm signal is triggered.

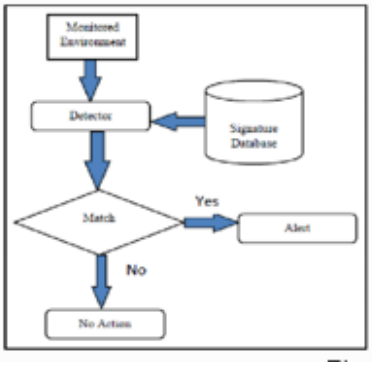

Figure 1.Signature-based intrusion detection system

Anomaly-based intrusion detection systems (AIDS)

Anomaly intrusion detection systems (AIDS) detects network/computer intrusions and misuses by means of classification system which run by machine learning that makes

activity normal or anomalous. This system creates standard of reliable activity and is to identify potentially spiteful traffic. Anomaly intrusion detection systems (AIDS) are used to detect unknown attacks.

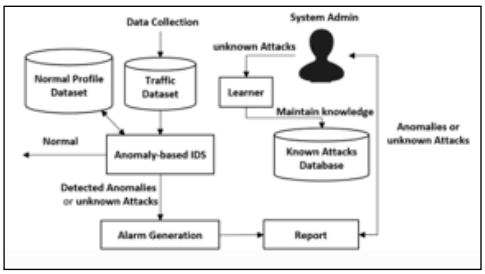

Figure 2.Anomaly-based intrusion detection system

The BoT-IoT Dataset

The BoT-IoT Dataset is a well-structured and representative dataset for training and validating the credibility of the systems. It incorporates legitimate and simulated IoT network traffic, along with various types of attacks. It would be evaluated the reliability of BoT-IoT dataset using different statistical and machine learning methods for forensics purposes compared with the benchmark datasets. This work provides the baseline for allowing Botnet identification across IoT specific networks. The BoT-IoT Dataset design a new realistic dataset that gives a detailed description of designing the test bed configuration and simulated IoT sensors.

Significance of Bot-IoT Dataset

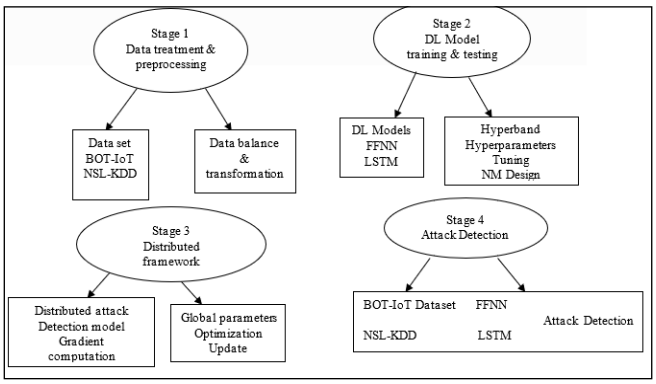

Figure 3.Bot-IoT Dataset

Bot IoT dataset is used to generate realistic data with the help of a cloud server consisting of Virtual Machines. The new IoT botnet dataset has a wider network and flow-based features. A flow-based Intrusion Detection System (IDS) can be examined and tested using flow-based features. Finally, we use different machine learning methods to test the accuracy of our proposed dataset. We also test the accuracy of our proposed dataset through various feature relationship and the methodology for recursive feature eradication. Our proposed IoT botnet dataset provides a ground to examine and evaluate anomalous activity detection model for IoT networks.

References

1. Khraisat A, Gondal I, Vamplew P, Kamruzzaman J, Alazab A. A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics. 2019 Oct 23;8(11):1210.
2. Singh A, Chatterjee K, Satapathy SC. An edge based hybrid intrusion detection framework for mobile edge computing. Complex & Intelligent Systems. 2022 Oct;8(5):3719-46.
3. Chilipirea C, Ursache A, Popa DO, Pop F. Energy efficiency and robustness for IoT: Building a smart home security system. In2016 IEEE 12th international conference on intelligent computer communication and processing (ICCP) 2016 Sep 8 (pp. 43-48). IEEE. .
4. Mohamed D, Ismael O. Enhancement of an IoT hybrid intrusion detection system based on fog-to-cloud computing. Journal of Cloud Computing. 2023 Mar 22;12(1):41.
5. Gyamfi E, Jurcut A. Intrusion detection in internet of things systems: a review on design approaches leveraging multi-access edge computing, machine learning, and datasets. Sensors. 2022 May 14;22(10):3744.
6. Govinda K, Prasad SK, Susheel SR. Intrusion detection system for smart home using laser rays. International journal for scientific research & Development. 2014;2(3):176-8.
7. Froiz-Míguez I, Fernández-Caramés TM, Fraga-Lamas P, Castedo L. Design, implementation and practical evaluation of an IoT home automation system for fog computing applications based on MQTT and ZigBee-WiFi sensor nodes. Sensors. 2018 Aug 13;18(8):2660.
8. Krishna IS, Ravindra J. Design and Implementation of Home Security Sytem based on WSNS and GSM Technology. International Journal of Engineering Science and Technology. 2014;2:139-42.
9. Bhargavi M, Kumar MN, Meenakshi NV, Lasya N. Intrusion detection techniques used for Internet of Things. Int. J. Appl. Eng. Res. 2019;14(24):4462-6.
10. Elrawy MF, Awad AI, Hamed HF. Intrusion detection systems for IoT-based smart environments: a survey. Journal of Cloud Computing. 2018 Dec;7(1):1-20.
11. Baig F, Beg S, Khan MF. Controlling home appliances remotely through voice command. arXiv preprint arXiv:1212.1790. 2012 Dec 8.
12. Meyer M, Hotter M, Ohmacht T. A new system for video-based detection of moving objects and its integration into digital networks. In1996 30th Annual International Carnahan Conference on Security Technology 1996 Oct 2 (pp. 105-110). IEEE.
13. Ramadan RA, Yadav K. A novel hybrid intrusion detection system (IDS) for the detection of internet

of things (IoT) network attacks. Annals of Emerging Technologies in Computing (AETiC), Print ISSN. 2020 Dec 20:2516-0281.

14. Zhao Y, Ye Z. A low cost GSM/GPRS based wireless home security system. IEEE Transactions on Consumer Electronics. 2008 May;54(2):567-72.
15. Z. Bing, G. Yunhung, L. Bo, Z. Guangwei and T. Tian, “Home Video Security urveillance”, Info-Tech and Infonet, 2001, Proceedings,ICII 2001-Beijing. 2001 International Conference, vol. 3, pp. 202-208.
16. Kale PV, Sharma SD. A review of securing home using video surveillance. Int. J. Sci. Res. 2014 May;3(5):1150-4.