IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11425

An Intrusion Detection System for Security in the IoT Environment

Dr. Jyoti Neeli[1], Bhargav HR[2], Chandan KS[3], Darpan NK[4] and Thanmai DL[5]

[1]Associate Professor, Department of Information Science and Engineering, Global Academy of Technology, Bengaluru

[2,3,4,5]Student, Department of Information Science and Engineering, Global Academy of Technology, Bengaluru

Abstract: IoT devices are getting increasingly popular. Several IoT issues highlight the necessity for IoT security. The number of assaults on these devices is growing, and most of them are minor variants of previously known attacks that can get beyond traditional firewalls. Existing systems are incompatible with IoT devices due to their low computing capability. Signature-based intrusion detection can only detect known patterns and attacks; therefore, it can't detect newer attacks with unknown patterns. Many systems also use cloud computing, which has the disadvantage of requiring constant internet access, as well as the fact that cloud services are frequently charged. The paper employed a Random Forest ML model to develop a real-time anomaly-based detection system. When a newer attack is detected that is not screened by the firewall, the anomaly-based intrusion detection system kicks in. It can handle newer/unknown assaults that signature-based systems cannot. We are also installing the IDS on a local, higher-powered device rather than using the cloud. The model developed using the IoT network traffic dataset generated by the IoT node in question.

Keywords - Intrusion Detection, Network Security, Anomaly Detection, Internet of Things.

I. INTRODUCTION

The Internet of Things, or IoT, is a network of interconnected "things" with unique identifiers and the ability to send and receive data without requiring human-to-human or human-to-computer interaction. These "things" could include computing devices, mechanical and digital machinery, as well as built-in sensors, monitors, and other electronic components. The security system adopted by various sites, which includes CCTV cameras, motion sensors, automated locks, smoke detectors, temperature sensors, and other IoT devices, is a good example of a network of IoT devices' devices are becoming increasingly common. They are widely employed in a variety of fields, and their utility is only going to grow. IoT devices aid in the automation of processes, the reduction of labour expenses, and the facilitation of smart living. As a result, it is critical to create a system that can ensure enough safety and security for IoT devices.

One such solution that may be used to make the IoT network as secure as feasible is an intrusion detection system. An intrusion detection system is a system that passively monitors data exchange in a network, as well as data exchange between the network and other organizations, for harmful activity that can be characterized as intrusions or attacks. The user is then notified, or a notification is sent to another system, which may or may not act against the discovered intruder. Simply described, an intrusion detection system is a CCTV camera if the network of devices is a home. An anomaly-based intrusion detection system is also a step up from just an intrusion detection system. This type of technology generates a profile of usual behaviour, and any activity that deviates from that profile is labelled as anomalous. A system based on anomalies is more equipped to defend against zero-day assaults. While developing this system, there are some problems that are unique to IoT devices. Low processing power and restricted resources (such as space/memory) are two examples. All these difficulties should be considered while designing the IDS system, and they should be addressed as quickly as possible.

II. LITERATURE REVIEW

In [1] The process of discovering a channel's weakness is known as intrusion detection. Snort, Eyebrows, and Hawkeye are just a few of the IDPS tools that have been created. The problem of false alarms, on the other hand, remains a difficult one to overcome. Noise can have a significant impact on the effectiveness of an intrusion detection system. Malicious packets created by software vulnerabilities, faulty DNS data, and escaped local packets could result in many false alerts. In this paper, researchers have suggested an IDS that is made up of four parts, (1) Signature Generator: The engine's main task is to use the training samples to develop signatures for several malicious activities. (2) Pattern generator: The engine at this layer processes diagnostic sessions, then turns each feature into a DNA series before recording it in a temporary database. (3) Intrusion detection engine: This is the most important component. The engine consists of a revolutionary pattern matching algorithm that analyses and compares the session DNA pattern with the signatures using certain present

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11425

real values and a set of arithmetic operations. (4) Output engine: In the post-analysis phase, the administrator will now be notified of the state of every session by defining whether it is regular-type or threat-type by generating several log files. Hence after assessing the false positive and false negative phenomenon, ample number of experiments were performed on NSLKDD dataset. It was found that as the number of samples in training dataset grows, so does the number of false positives. In [2] The detection of anomalies in actual streaming data is a popular issue in data analytics right now. They addressed this problem in this work with the purpose of discovering irregularities in data on humans, particularly fall. The suggested system will use wearable sensors to collect real-time physical activity data, recognise fall as an out-of-the-ordinary sequence in the statistics, and notify the tracking system to take suitable measures in case of a fall. It could be beneficial for tracking elderly people in hospitals and in nursing homes. MLP is used to implement the suggested system's ML model. This has gained higher accuracy for categorization between fall and non-fall using MobiAct which is a freely available dataset. As a part of future work, they intend to examine the IBM tools' usefulness and performance utilized in their framework. In [3] A unique and intelligent three-layer IDS architecture is given in this research. The IDS proposed here covers three key functionalities to overcome the limitations of current systems they are, (1) recognise the type of IoT device linked to the network and profile its typical behaviour, (2) identify wireless attacks on IoT devices that are linked, & (3) classify the type of assault which is being used. To assess the effectiveness of using a supervised machine learning method to automate every function, network activity data from a realistic testbed having a variety of widely viable and renowned IoT devices was collected. The performance of systems 3 core functions results in achieving greater accuracy and F1 scores were also obtained. As a result, the suggested architecture demonstrates that it can successfully identify among IoT devices on the network, identify if the behaviour on the network is fraudulent or not & find out which threat was executed over which associated device automatically. All assets here are open to the research community and can be used to support future research into various elements of IoT. The system will need to be deployed in real-time in the future because it can be used in real-world, diverse IoT and Industrial IoT situations. In [4] E-Spion, a system-level IDS tailored for IoT devices. E-Spion uses system data to create a three-layer compatible profile for IoT devices that consists of varied extra cost for IoT devices that are connected to system information and identifies attacks based on unusual behaviour. By using an effective device - a modular three-layered design, E-spion is particularly intended for risky IoT devices. E-Spion was thoroughly examined with a comprehensive collection of 3973 IOT malicious software samples and resulted in good detection rates which were found for 3 layers of detection. The goal of this paper is to develop more extensive device behaviour profiles & give more fine-grained detection. In [5] They have proposed EDIMA. Using machine learning classification techniques, EDIMA is a solution for early identification of network behaviour that originated from IoT infectant. Existing IoT malware was classified into several types based on the software defencelessness it targeted. The categorization performance of EDIMA was evaluated using a testbed that included a Personal Computers, mobile phones & IOT device linked to a gateway for accessing. Now at accessible gateway level, feature vectors were constructed from packet traffic specimens. Following that, the predominance of benign and harmful traffic feature vectors for distinct malware types was illustrated. A subset of the recovered feature vectors was utilized as training data for a few common machine learning techniques, and The Machine Learning models were then used to classify test data, and the results were reported.

The authors in [6] demonstrate how to utilise an Artificial Neural Network (ANN) to analyse network traffic in sequences in the IoT environment in order to diagnose faulty activities. They have used classification accuracy to establish the validity of the used method. They've also proven the validity of their method by demonstrating classification accuracy. When the dataset was used for training and testing, the accuracy was improved. The ANN classifiers detected malicious IoT nodes with a success rate of 77.51 percent. Furthermore, they assessed and built a threat model to identify potential hostile assaults. However, these are just speculations at this point. They intend to diversify the devices utilized in the research process in the future. In [7] They created a model based on intrusion detection in two levels for detection purpose on IOT networks in this research. The first-level model is a flow-based approach for identifying anomalous activity that differentiates between regular and aberrant input patterns. The flow will be transmitted to the second level model if it is found to be abnormal, which will thoroughly investigate the flow and classify the observed anomaly. RFE is used for feature selection in the level-2 model, and SMOTEENN is used to balance the dataset. After testing F scores were obtained as result. They intend to measure the construct in a realistic scenario in the future to improve its validity. In [8] they have proposed an IDS security framework to provide IoT network customers with independent and comprehensive security agencies. They have created a foundation for a self-contained IDS that employs machine learning methods to detect unusual network activities. They'll be able to retain security while achieving clever connectivity, thanks to the system's ability to integrate into any network, allowing them to realize their goal of safe computing that is accessible to everyone. A prototype IID was in developing stage which will be used to compare the detecting modules to a variety of IoT-specific security threats. The detection module for machine learning will be evaluated and strengthened in the future to allow an IoT network, more precise detection of anomalies. [9] Discovering IoT malware is becoming a more pressing concern as the Internet infrastructure and personal data become more vulnerable. This research investigated recently identified IoT threats as well as stable detection methods. IoT attack detection approaches can be classified into two groups, non-graph based, and graph based, depending on a few strategies and strengths and shortcomings of current IoT malicious fixed

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11425

detection. When identifying basic and forthright malware without customisation or discombobulation, non-graph-based approaches can produce satisfactory results. Graph-based approaches have the capacity to reliably discover invisible or intricate malicious code despite their complexity when examining the sequence control of IoT spyware. To compare the results of these research, they used the same IoT dataset with 11200 samples to deploy and analyse them, as a result an average of 90 percent accuracy was obtained. As a part of future work, a graph-based lightweight detection approach that will aid in the identification of IoT systems require the development of spyware files. In [10] Passban is an anomaly-based Intrusion Detection System developed to be hosted and operated by a standard edge device. Firstly, they have built an IoT testbed that may be configured to seem like a conventional smart home automation setup. Then, to test the suggested IDS's performance, they have set up the IoT testbed as two different scenarios. In the first scenario, IDS is installed, and it is made to run on the IoT gateway; at this point of time, passban may defend the gateway as well as the other IoT devices that are linked directly to it. In the second scenario, passban is given as a different additional device that is not connected to the network for which it is designed to safeguard: here, it can track the entering and leaving traffic of the IOT device's network which is connected to the gateway and scan it to identify suspicious patterns. The most appealing aspect of the suggested IDS is its ability to train itself, utilizing legal flows in the traffic from the targeted IOT network with the help of simple one-class classification machine learning methods. Regarding threat accuracy rate, the research revealed that when using iForest, Passban IDS can get F1 scores more than 0.9 on various assaults.

III. LITERATURE REVIEW SUMMARY

The summary of literature review is depicted in the table

Sl. No	Citation	Year	Methodology	Pros	Cons
1	Shashwat Vikram, et Al [10]	2018	For recognising and preventing various types of assaults, they suggested a four-layered architecture: Signature generator, Pattern generator, Intrusion detection engine, and Output layer	The proposed IDS's simulation result shows that further research on this topic has a bright future.	As the number of samples grows in the training dataset, the false positive rate also increases.
2	Haruna, et Al [7]	2018	They present a deep learning model for detecting falls, and they evaluate their system using two datasets. MobiAct was chosen for having the most subjects, while SisFall was chosen for having the most actions.	The test resulted in a 98.75 percent accuracy. This demonstrates that the generated model is effective and may be used to further build the suggested system.	To characterize different sorts of falls, the model must be expanded. While connecting and ingesting data from many IoT devices, the framework's scalability and performance must be validated.
3	Lowri Williams, et Al [9]	2019	The first layer of the utility will scan the network for interconnected Devices and identify them using their MAC addresses. The same packets are classified as benign or dangerous at the second layer. The third layer will classify infected files as one of their key attack categories if the second layer discovers them.	The F-measures for the system's three essential functions are 96.2 percent, 90.0 percent, and 98.0 percent, correspondingly. The system has all the necessary tools to detect an assault.	The system must be implemented in real-time. Advance techniques need to be implemented to cover more complex attacks.
4	Puneet Sharma, et Al [1]	2019	E-Spion is made up of three layers, each of which employs three different types of device logs derived from three separate sources.	The detection rate for the PWM layer was 79.09%. We can easily see that the simple PWM can detect the majority of IoT malware variants	False detection rates are found in the PWM layer which can be reduced. The device logs must be broadened; this can be

DOI: 10.17148/IJARCCE.2022.11425

			PWM, PBM, and SBM are the three detection modules in their anomaly detection engine	simply by white-listing process names. The detection rate of the PBM layer is 97.02 percent. SBM layer has a 100% detection rate and no false positives. This is the detecting module with the most granularity.	done by including network logs of the device.
5	Teng Joon Lim, et Al [3]	2019	EDIMA is a suggested technique for detecting scanning packet traffic created by IoT malware using machine learning algorithms. It's built with an architecture that includes five separate modules.	F1 scores of 0.86,0.96,0.92 were obtained when the trained algorithms were tested using test data of the three malware categories.	The performance assessment of EDIMA is still in the work. Further training of machine learning algorithms is required.
6	N. Chowdhury, et Al [4]	2019	They have used and compared the results of many supervised methods, including ANN classifiers, and measured the results of the chosen techniques using their dataset.	Malicious nodes may be discovered with an accuracy of 77.51 percent. More data accuracy may be acquired when the size of the training data is raised. As a result, the proposed approach is ideal for all purposes.	A key constraint is the number of Smart bulbs or IoT devices that can communicate over Wi-Fi. As a result, additional IoT-related technologies such as Zigbee or Zwabe were unavailable.
7	I. Ullah, et Al [5]	2019	To pick ideal features for precision, the methodology used here is RFE approach and deep packet inspection.	Intrusion Detection model split into two models - Level 1 and Level 2 for detection and deep inspection respectively. 100 percent precision was achieved.	Implementation & validation of the models needs to be done.
8	S. Chawla, et Al [6]	2019	Virtual Network Connection module, Data Collection and Transformation module	The suggested data collection and conversion technique can reduce the quantity of the gathered network traffic, allowing the IID to operate inaudibly anywhere within the host network's service area.	Evaluating and improving the machine learning detection module so that anomalies in an IoT network may be identified with greater accuracy.
9	H. Nguyen, et Al [8]	2020	They used static features such as control flow graphs, operation codes, texts, file headers, Gray-scale images, and so on. IoT malware detection algorithm's accuracy and complexity are strongly influenced by how these features were retrieved and processed.	Even though roughly 2000 malware samples out of a total of 7000 samples are unable to read and calculate the file header, The technique used here generated an accuracy greater than 99 percent for every algorithm.	When detecting unknown malware, the non-graph technique may lose accuracy. It is necessary to create and develop a graph-based lightweight detection method that will aid in the identification of malicious executable files in IoT devices.
10	Z. Janjua, et Al [2]	2020	Passban employs the learnt model to detect unusual occurrences in incoming network data after the training phase. To apply machine learning techniques to the data, several features (such as max fpktl, mean active, and	On various assaults, passban IDS can get F1 scores of better than 0.9. In terms of resource utilization, they have proven that Passban can be executed even on cheap IoT gateway boards.	False alarm rate diminishes the system performance and reduces the system's overall reliability. Hence this must be kept to a minimum.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11425

			24 other important features) were retrieved.		

IV. PROPOSED METHODLOGY

As shown in Figure [1]. [3] The system is based on an already existing IDS (Intrusion Detection System) that tries to defend the home-network from assaults and invasions. We're integrating these pre-existing models to get more benefits while minimizing the drawbacks. There is a huge scope for research to create an IDS for IoT devices as only few trials have been made to create one. The market does have a few IDS systems, but they cater to non-IDS networks. Core principles of IDS systems are taken into consideration and are being modified as per the requirement.
For intrusion detection, the machine learning model random forest will be employed. The network data collected during runtime will be pre-processed and given to the model. The network data will undergo a deep packet inspection after which the information obtained will be examined and classed as normal or abnormal (Anomalous).

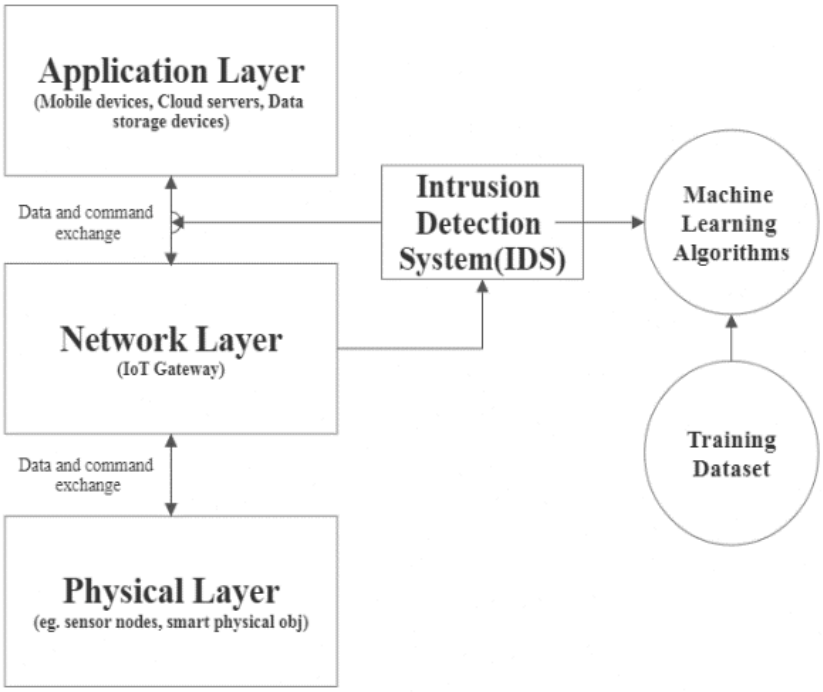

Figure 1: Proposed Methodology

V. CONCLUSION

An IDS (Intrusion Detection System) which is developed for IoT devices in a network can be leveraged to increase security in real time. After the firewall, it serves as an additional layer of protection against any kinds of intrusion. The main goal is to detect intrusions in real time by effectively analysing and classifying network traffic. The paper provides a survey of a few of the different types of intrusion detection systems such as anomaly or signature-based systems. The proposed methodology uses the random forest machine learning algorithm which targets to improve the accuracy and the detection of a broad variety of attacks.

REFERENCES

[1] Sheikh, Nazim Uddin, Hasina Rahman, Shashwat Vikram, and Hamed AlQahtani. "A Lightweight Signature-Based IDS for IoT Environment." arXiv preprint arXiv:1811.04582 (2018).
[2] Mahfuz, Sazia & Isah, Haruna, “Detecting Irregular Patterns in IoT Streaming Data for Fall Detection”, BOOK: 2018/11/15.

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.11425

[3] Anthi, Eirini, Lowri Williams, Małgorzata Słowińska, George Theodorakopoulos, and Pete Burnap. "A supervised intrusion detection system for smart home IoT devices." IEEE Internet of Things Journal 6, no. 5 (2019): 9042-9053.

[4] Mudgerikar, Anand, Puneet Sharma, and Elisa Bertino. "E-spion: A system-level intrusion detection system for iot devices." In proceedings of the 2019 ACM Asia conference on computer and communications security, pp. 493-500. 2019.

[5] Kumar, Ayush, and Teng Joon Lim. "EDIMA: Early detection of IoT malware network activity using machine learning techniques." In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pp. 289-294. IEEE, 2019.

[6] M. A. Khatun, N. Chowdhury and M. N. Uddin, "Malicious Nodes Detection based on Artificial Neural Network in IoT Environments," 2019 22nd International Conference on Computer and Information Technology (ICCIT), 2019, pp. 1-6, doi: 10.1109/ICCIT48885.2019.9038563.

[7] I. Ullah and Q. H. Mahmoud, "A Two-Level Hybrid Model for Anomalous Activity Detection in IoT Networks", Consumer Communication and Networking Conference (CCNC), 2019.

[8] S. Chawla and G. Thamilarasu, "Security as a service", Proceedings of the Fifth Cybersecurity Symposium, 2018. Available: 10.1145/3212687.3212872.

[9] Q. Ngo, H. Nguyen, V. Le and D. Nguyen, "A survey of IoT malware and detection methods based on static features", ICT Express, vol. 6, no. 4, pp. 280-286, 2020. Available: 10.1016/j.icte.2020.04.005.

[10] M. Eskandari, Z. Janjua, M. Vecchio and F. Antonelli, "Passban IDS: An Intelligent Anomaly-Based Intrusion Detection System for IoT Edge Devices", IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6882-6897, 2020. Available: 10.1109/jiot.2020.2970501

