Machine Learning Based Network Security In Internet Of Things

Pranav Pankhawala[1]*, Dr Sumedha Sirsikar[2]

*[1] PG student of MTech Network Management and Cyber Security School of Computer Engineering and Technology, Dr Vishwanath Karad MIT World Peace University, Pune,
E-mail:- pranav.pankhawala@gmail.com
[2] Associate Professor at School of Computer Engineering and Technology, Dr Vishwanath Karad MIT World Peace University, Pune, E-mail:-sumedha.sirsikar@mitwpu.edu.in
***Corresponding Author: -** Pranav Pankhawala

Abstract:

The adoption of IoT has accelerated integration and expanded the reach of the Web beyond computers, tablets, and smartphones to a variety of physical objects. This is being driven ahead by the Internet of Things, which is starting to ingrain itself more deeply into daily life. While IoT devices offer several creative features and make life simpler, they also greatly increase the possibility for nefarious people, criminal organisations, and maybe even governments to spy on and meddle with unaware IoT system users. Demand for data science approaches to tackling these issues has increased as the coming crisis gets worse, and new study demonstrates that predictive analytics taught with ml algorithms offer tremendous promise.

Keywords: Network Security; Threat; Machine Learning; Security Analysis; Internet of Things

DOI Number: 10.14704/nq.2022.20.9.NQ440121 **Neuro Quantology 2022; 20(9):1078-1082**

I. OVERVIEW

The necessity to defend IoT devices against different assaults increases along with the adoption of these devices. They not only provide weak edge hardware, but also weak entry points that leave the remainder of the network open to intrusion.

The many attack types and mitigation strategies are covered in this essay.

IoT devices need to be regularly updated and watched over to stave against attackers.

II. INTRODUCTION

IoT security has emerged as a prompt and important matter that necessitates plausible work from scientific community. IoT security has become an urgent issue that requires the scientific community to do some logical effort. Determining this need network security for IoT networks is the main objective of this article, which also seeks to identify study gaps in previous works on attack detection and mitigation.

IoT is a term utilised to define internet systems that can detect and regulate their environment with next to no human intervention. These devices are used in many industries, such as critical networks, homes, smart cities, businesses, medical services, manufacturing, and education. The main factor for IoT's mass acceptance is that such tools help to increase our everyday routines by collecting data via sensors or by influencing our surroundings via actuators.

On the market, there's a growing number of unsecure devices. Many integrated systems can be discovered by using search engines like Shodan., and sites such as Insecam document publicly available and susceptible systems, enabling their weaknesses to be abused at scale. A huge IoT botnet consisting of multitudes of compromised IP-cameras launched a DDoS attack against Dyn, a major DNS provider. Inside and outside hackers can just use IoT devices which it reveals TCP/UDP ports to random local end devices within one residence or organisation, and virtual organisations on the Internet In general, to mirror malicious activities and infiltrate [1].

III. LITERATURE REVIEW

To reduce IoT-related cyber-attacks, security must be evaluated at all levels of IoT networks (manufacturers, users, and service providers).

Manufacturers are hesitant to conduct security audits on their products because it costs money. Although it is expected that manufacturers adhere strictly to software development principles and take security seriously, many unsecured devices are released into the market. This is due to the desire of manufacturers to launch their own low - cost products and before the of their competitors. The main reason why makers don't really assess their product lines is an absence of cybersecurity skills. They are mostly undertrained to evaluate these products before they are released. Therefore, as consequence, insecure IoT devices enter the market. The chief factor manufacturers don't really test their own products is for financial reasons. Some such makers have already been alleged of failure to respond to vulnerabilities after their products were released, leaving them vulnerable.

The primary reason cyberthreats involving IoT systems continue to happen is due to users' ignorance. Network managers, estate managers, and residential consumers must preferably follow the standard acquisition process and install tested devices on their networks. Household consumer device manufacturers doesn't provide details about potential threats and functionalities of their products. These devices' user guides don't get into extensive detail about security. Such products are usually tested on an institutional level, and they are also prone to cyber. This could be because the checking conducted prior to approval was insufficient. Inadequate testing may lead in the misrepresentation of a critical vulnerability.

Although these systems were thoroughly tested before purchase, subsequent upgrades may start introducing newer vulnerabilities. To tackle these issues, systems should be tested on a regular basis when in use. Furthermore, due to limited capabilities, IoT devices unable to do conventional analytical entities to keep their situation posted. Without solutions, attackers can roam the network freely and undetected. It is difficult for household owners to keep track of events on IoT devices due to limited monitoring capabilities when compared to an organisation that employs engineers and cyber experts. ISPs can address such issues by providing internet solutions for monitoring and control internet activity. Government agencies and regulatory are working to develop standards and guidelines to maintain IoT devices secure.

The US Senate decided to introduce the IoT Cybersecurity Improvement Act of 2019 that proposes a minimum baseline security standard for government agencies to consider when purchasing devices. NIST and ENISA have recommended minimum cybersecurity standards for IoT device security functionalities including key management and authorization.

Since IoT systems have limited resources, network level protection is preferable to device level protection. Security mechanisms, intrusion detection and prevention systems (IPS) are widely used to determine malicious network activity.

Since IoT devices are diverse, it is complicated for these solutions to distinguish between malicious and benign IoT traffic activity. Besides, with multitudes of IoT devices linked, individually monitoring each device does become difficult and expensive. Malicious actors have a very appealing attack target because of scale of IoT deployments. Finding and abusing a weakness can easily create a huge army of attackers, that can then be used to launch additional attacks. Inadequate screening of IoT devices, inadequate physical security on campus, unsatisfactory authentication mechan- isms, and insufficient privacy design are some widespread drawbacks of IoT deployments. For years, machine learning has been proposed to solve network security concerns. Moskovitch indicated an accuracy of more than 90% in predicting worm activity in 2007 and was granted a patent in 2013. Various approaches to dealing with such attacks have been proposed since Stuxnet.

Despite their diversity, IoT systems are susceptible to attack since they heavily rely on Internet access for communication and information transfers. A wide range of attacks can be launched against an IoT system. For example, worms replicate and spread across a whole network. Denial of Service restrict access to a subset or even the entire network. Eavesdropping is a communication intercepting technique [1].

In 2013, the CIA triad has been enlarged to the IAS octave. It incorporates concepts such as accountability, verifiability, trustworthiness, non-repudiation, and privacy. Accountability means having the power to make users answerable for their deeds. The term "auditability" describes the capacity to keep an eye on and compile reports on system activity. The trusting third parties is a sign of trustworthiness.

IV. METHODOLOGY

We took a machine learning-based approach to this issue. We may train these models to detect malicious packets travelling via networks using techniques such neural networks, random forests, and k-nearest neighbours.

These distinguish between malicious and good packets using protocol names and a number of other factors. To train and validate these algorithms, we used one 1.8GB datasets with several thousand entries and about 80 attributes. Following training and testing, we graph the accuracy, recall, and other factors that can be used to determine whether or not a particular packet was malicious.

The information is read as a data frame using the Panda package. Additional libraries such as sklearn, seaborne, NumPy, and others were utilised to divide the data into training and testing portions. Models were created using decision trees and random forests as classifiers. The models were given parameters such as maximum depth, maximum features, and estimators. To plot the features and trees, we utilised the Matplotlib library.

The nearest 3,5,7,11, & 21st neighbours were utilised to train the model in the KNN algorithm. To improve accuracy, Manhattan and Euclidean distances were used. 30 percent testing points and 70 percent training points were assigned to the dataset. The split ratio could be changed to achieve different levels of precision.

V. Results

There are total 4 performance metrics based on which we can conclusively say if the said model is well trained or not.

The proportion of correctly identified positive samples (True Positives) to all identified positive samples is known as precision (either correctly or incorrectly). Precision enables us to see how reliable the machine learning model is at classifying the model as positive.

Divide the total amount of positive data by the percentage of samples tested that were clearly predicted as such to calculate recall. The recall of the model measures how that can recognise positive samples. As more samples are identified, the recall rises.

Recall and accuracy are combined in a single value. The F1-score compensates for both FPs and FNs since it takes accuracy and recall into consideration. Precision and recall increase in proportion to the F1 score. The F1-score is between 0 and 1. The model is more accurate the closer it is to one.

Support may be shown by the proportion of measures of the true response that falls within each category of desired values.

Figure 5.1 demonstrates that the precision and recall numbers are routinely higher than 95%. We conclude from these results that now the "support" feature supports the capacity to assess whether a particular packet appears to be dangerous or not. Support can essentially be measured as the proportion of instances of the legitimate response which thus fall within each category of goal values.

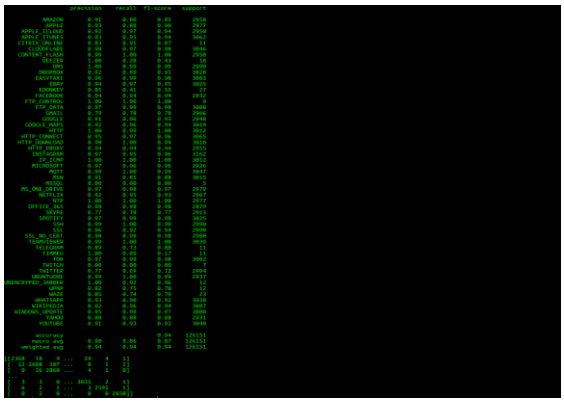

Fig 5.1 K-Nearest Neighbours results

Figure 5.2 demonstrates that the precision and recall numbers are routinely higher than 95%. We conclude from these results that now the "support" feature supports the capacity to assess whether a particular packet appears to be dangerous or not. Support can essentially be

measured as the proportion of instances of the legitimate response which thus fall within each category of goal values.

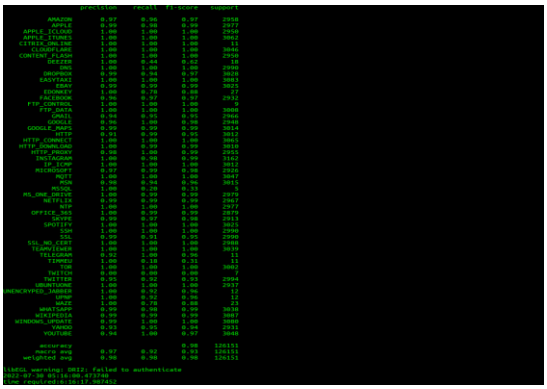

Fig 5.2 Random Forest Results

VI CONCLUSION AND FUTURE SCOPE

Network security is a broad and complex subject. It is the need of the hour that proactive network protection be implemented to minimize damage caused by threat actors. IoT is a concept that is beginning to materialize. Not only is it necessary to protect computer networks from attacks but special emphasis should be put on IoT network security as these devices are currently the most vulnerable part of networks and rigorous security policies should be developed to keep these devices secured.

As time goes on, IoT networks will support a variety of technologies. IoT systems are anticipated to number in the billions by the end of the decade. As deployment of Iot systems increases, security has become increasingly crucial in order to protect data and sustain data flow.

Future development on the project will entail implementing endogeneity bootstrap and licensing utilizing a Blockchain to mitigate a DNS issue. Additionally, analytics might be implemented to assess edge device usage and physical manipulation. Edge devices can be strengthened to resist tampering.

Future work may involve developing and evaluating characteristics that are meant to identify specific characteristics of various attack types as well as information security risks for the evaluation of attacks that are not yet known to exist. Future research will also need to put more emphasis into evaluating machine learning strategies for anticipating attacks on IoT application layer that were not included in this study. Analysing how well "stateless" traits perform in attack detection might be interesting. Evaluating the effectiveness of even more machine learning techniques, such as deep learning, would also be intriguing.

References

A. Burg, A. Chattopadhyay and K. -Y. Lam, "Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things," in Proceedings of the IEEE, vol. 106, no. 1, pp. 38-60, Jan. 2018, doi: 10.1109/JPROC.2017.2780172.

Xiao, Min & Guo, Mei. (2020). Computer Network Security and Preventive Measures in the Age of Big Data. Procedia Computer Science. 166. 438-442. 10.1016/j.procs.2020.02.068.

Hamza, Ayyoob & Habibi Gharakheili, Hassan & Sivaraman, Vijay. (2020). IoT Network Security: Requirements, Threats, and Countermeasures https://doi.org/10.48550/arXiv.2008.09339

A. Kim, J. Oh, J. Ryu and K. Lee, "A Review of Insider Threat Detection Approaches With IoT Perspective," in IEEE Access, vol. 8, pp. 78847-78867, 2020, doi: 10.1109/ACCESS.2020.2990195.

K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," in IEEE Access, vol. 8, pp. 88892-88932, 2020, doi:10.1109/ACCESS.2020.2993553.

Wheelus, C.; Zhu, X. IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework. IoT 2020, 1, 259-285. https://doi.org/10.3390/IoT1020016

K. Tange, M. De Donno, X. Fafoutis and N. Dragoni, "A Systematic Survey of Industrial IoT Security: Requirements and Fog Computing Opportunities," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2489-2520, Fourthquarter 2020, doi: 10.1109/COMST.2020.3011208.

M. Asplund and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services," in IEEE Access, vol. 4, pp. 2130-2138, 2016, doi: 10.1109/ACCESS.2016.2560919.

M. Bagaa, T. Taleb, J. B. Bernabe and A. Skarmeta, "A ML Security Framework for Iot Systems," in IEEE Access, vol. 8, pp. 114066-114077, 2020, doi: 10.1109/ACCESS.2020.2996214.

Y. K. Saheed and M. O. Arowolo, "Efficient Cyber Attack Detection on the Internet of Medical Things-Smart Environment Based on Deep Recurrent Neural Network and ML Algorithms," in IEEE Access, vol. 9, pp. 161546-161554, 2021, doi: 10.1109/ACCESS.2021.3128837.

S. Latif et al., "Intrusion Detection Framework for the IoT Using a Dense Random Neural Network," in IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6435-6444, Sept. 2022, doi: 10.1109/TII.2021.3130248.

H. Wu, H. Han, X. Wang and S. Sun, "Research on Artificial Intelligence Enhancing IoT Security: A Survey," in IEEE Access, vol. 8, pp. 153826-153848, 2020, doi: 10.1109/ACCESS.2020.3018170.

N. Mishra and S. Pandya, "IoT Applications, Security Challenges, Attacks, Intrusion Detection, and Future

Visions: A Systematic Review," in IEEE Access, vol. 9, pp. 59353-59377, 2021, doi: 10.1109/ACCESS.2021.3073408.

D. Wei et al., "Dataflow Management in the IoT: Sensing, Control, and Security," in Tsinghua Science and Technology, vol. 26, no. 6, pp. 918-930, Dec. 2021, doi: 10.26599/TST.2021.9010029.

M. Azrour, J. Mabrouki, A. Guezzaz and Y. Farhaoui, "New enhanced authentication protocol for IoT," in Big Data Mining and Analytics, vol. 4, no. 1, pp. 1-9, March 2021, doi: 10.26599/BDMA.2020.9020010.

S. Siboni et al., "Security Testbed for Internet-of-Things Devices," in IEEE Transactions on Reliability, vol. 68, no. 1, pp. 23-44, March 2019, doi: 10.1109/TR.2018.2864536.

R. Sardar and T. Anees, "Web of Things: Security Challenges and Mechanisms," in IEEE Access, vol. 9, pp. 31695-31711, 2021, doi: 10.1109/ACCESS.2021.3057655.

N. M. Allifah and I. A. Zualkernan, "Ranking Security of IoT-Based Smart Home Consumer Devices," in IEEE Access, vol. 10, pp. 18352-18369, 2022, doi: 10.1109/ACCESS.2022.3148140.

S. Zaman et al., "Security Threats and Artificial Intelligence Based Countermeasures for IoT Networks: A Comprehensive Survey," in IEEE Access, vol. 9, pp. 94668-94690, 2021, doi: 10.1109/ACCESS.2021.3089681.