International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

A Lightweight Intrusion Detection System for the Internet of Things Based on Machine Learning

Ms.M.ANITHA[1], Mr.CH.SATYANARYANA REDDY[2], Ms.P.JAYASRI

#1 Assistant professor in the Department of Master of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District

#2 Assistant professor in the Department of Master of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR(DT)

#3 MCA student in the Department of Master of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District.

Abstract_ The Internet of Things (IoT) is particularly susceptible to attacks due to the prevalence of cheap, widely distributed low-powered computing devices. The goal of this study is to strengthen the security of the Internet of Things (IoT) by creating a lightweight intrusion detection system (IDS) based on two machine learning techniques: feature selection and feature classification. The filter-based method was utilised to choose the characteristics because of its minimal computational cost. Our system's feature classification strategy was determined through an analysis of many methods, including naive Bayes (NB), decision tree (DT), random forest (RF), k-nearest neighbour (KNN), support vector machine (SVM), and multilayer perceptron (MLP). Last but not least, the DT technique was picked for our system because of its stellar performance across different datasets. The research results can be used as a benchmark for vetting potential feature selection methods in the field of machine learning.

Keywords:
Internet of Things (IoT), intrusion detection system (IDS), anomaly detection, feature selection

1.INTRODUCTION

Insecure and unfavourable deployment environments are common for IoT devices, making them more vulnerable to a variety of attacks [3]. As a result, security measures are essential for protecting Internet of Things devices from malicious attacks. An Intrusion Detection System (IDS) is a tool for monitoring attacks on a computer or network by analysing the attacker's actions and patterns [4]. It can be used as a secondary defence against potential attackers [5]. An IDS's primary goal is to detect as many attacks as possible with sufficient precision while decreasing power usage within acceptable limits [6]. One can choose between a signature-based IDS or an anomaly-based IDS. When a signature-based IDS, sometimes called a misuse-based IDS, is in place, it is able to spot intrusions by comparing newly gathered data to an existing knowledge base or signatures of known attacks. While this method is effective at finding recognised threats, it is often blind to unknown ones. In order to identify significant outliers, anomaly-based intrusion detection systems compare

typical actions to those that have been predetermined.

Numerous studies have been conducted recently in the fields of IoT and IDS in order to provide the desirable safety mechanism. A light anomaly detection method predicated on the idea of the sport theory piqued the interest of Sedjelmaci et al. [3]. In order to foresee the equilibrium condition that allows the IDS agent to recognise a new attack's signature, the authors rely on the Nash equilibrium. Using the K-Nearest Neighbor (KNN) classification technique in a wireless sensor network, Li et al. [7] suggested a new intrusion detection machine. The gadget can make a flood attack on a wifi sensor network a reality. It also does experiments to see what happens during a flood attack. When it comes to the IoT, Thanigaivelan et al. [8] proposed an anomaly detection device that can be distributed internally. Monitoring, ranking, isolating, and reporting are the primary functions of the device. At one hop, nodes reveal and become aware of their neighbours; if a neighbour no longer maintains the required rating, the neighbour is marked as an outlier. In the IoT, Shahid Raza [4] proposed a device called SVELTE for real-time intrusion detection. Integrated into the Contiki operating system is a powerful IDS that may be used to protect your network from unwanted intruders. This approach can only detect network-based attacks like as content spoofing, gulp, and selective switch. For small IoT devices, Douglas et al. [9] presented a lightweight deep-packet anomaly detection approach. The method use n-gram bit-patterns to simulate payloads, with the n-gram size being freely adjustable across dimensions.

2.LITERATURE SURVEY

2.1 Atzori, L., Iera, A., Morabito, G. (2010). The Internet ofThings: A survey. Computer Network, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.

2.2 **Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016).Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology.IEEE ICC - Mobile and Wireless NetworkingSymposium.**

https://doi.org/10.1109/ICC.2016.7510811

In the Internet of Things (IoT), resources' constrained tiny sensors and devices could be connected to unreliable and untrusted networks. Nevertheless, securing IoT technology is mandatory, due to the relevant data handled by these devices. Intrusion Detection System (IDS) is the most efficient technique to detect the attackers with a high accuracy when cryptography is broken. This is achieved by combining the advantages of anomaly and signature detection, which are high detection and low false positive rates, respectively. To achieve a high detection rate, the anomaly detection technique relies on a learning algorithm to model the normal behavior of a node and when a new attack pattern (often known as signature) is detected, it will be modeled with a set of rules. This latter is used by the signature detection technique for attack confirmation. However, the activation of anomaly detection for low-resource IoT devices could generate a high-energy consumption, specifically when this technique is activated all the time.

2.3 Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultralightweight deep packet anomaly detection for Internet of Things devices. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC). https://doi.org/10.1109/PCCC.2015.7410342

As we race toward the Internet of Things (IoT), small embedded devices are increasingly becoming network-enabled. Often, these devices can't meet the computational requirements of current intrusion prevention mechanisms or designers prioritize additional features and services over security; as a result, many IoT devices are vulnerable to attack. We have developed an ultra-lightweight deep packet anomaly detection approach that is feasible to run on resource constrained IoT devices yet provides good discrimination between normal and abnormal payloads. Feature selection uses efficient bit-pattern matching, requiring only a bitwise AND operation followed by a conditional counter increment. The discrimination function is implemented as a lookup-table, allowing both fast evaluation and flexible feature space representation. Due to its simplicity, the approach can be efficiently implemented in either hardware or software and can be deployed in network appliances, interfaces, or in the protocol stack of a device. We demonstrate near perfect payload discrimination for data captured from off the shelf IoT devices

3.PROPOSED SYSTEM

One of our key objectives is for the IDS to be light and adapt to the processing capabilities of the restricted nodes. Because of the restricted processing capability and power consumption, it is not practical to have an active intrusion detection agent in each node of an IoT, according to [20]. As a result, we've established a centralised IDS architecture to address the issues of limited capacity on the one hand and peripheral heterogeneity on the other, with the IDS being built above the Gateway component on the network layer of the IoT. The activity diagram for our Lightweight Intrusion Detection System (LIDS), which detects intrusions by observing current behaviour and comparing it to expected behaviour.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

An alarm will be triggered if there is a difference between the two behaviours. There are three phases to it.

In this paper author is building light weight intrusion detection system for IOT networks using machine learning algorithms. Author has evaluated performance of various machine learning algorithms such as SVM, Random Forest, Decision Tree, Naïve Bayes, KNN and Multilayer Perceptron and in all algorithms Decision Tree and KNN is giving better performance. To reduce training time author is using filter based features selection algorithm which will select important attributes from training dataset and the attributes whose correlation value is less than given threshold will be removed out.

To implement this project author has used 3 datasets such as KDDCUP, NSLKDD and UNSW_NB15 and this dataset contains various attacks as Denial of Service, R2L, U2R, Probe and many more. Other details can be read from paper.

Figure 2 shows the activity diagram of our Lightweight Intrusion Detection System (LIDS) that consists in detecting an intrusion by observing the current behavior and comparing it to the normal behavior. If there is a deviation between the two behaviors, an alarm will be triggered. It is composed of three phases:

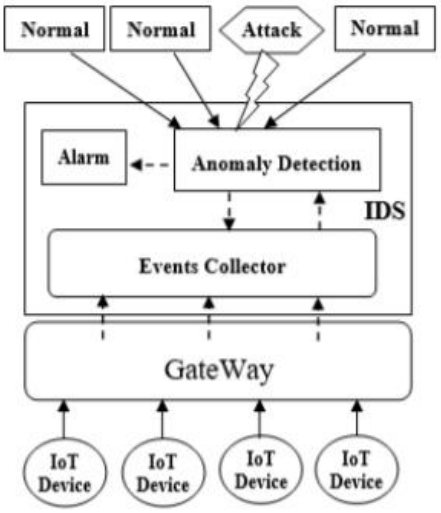

Fig 1:LIDS Architecture Model

4.RESULTS AND DISCUSSIONS

In this paper author is building light weight intrusion detection system for IOT networks using machine learning algorithms. Author has evaluated performance of various machine learning algorithms such as SVM, Random Forest, Decision Tree, Naïve Bayes, KNN and Multilayer Perceptron and in all algorithms Decision Tree and KNN is giving better performance. To reduce training time author is using filter based features selection algorithm which will select important attributes from training dataset and the attributes whose correlation value is less than given threshold will be removed out.

To implement this project author has used 3 datasets such as KDDCUP, NSLKDD and UNSW_NB15 and this dataset contains various attacks as Denial of Service, R2L, U2R, Probe and many more. Other details can be read from paper.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

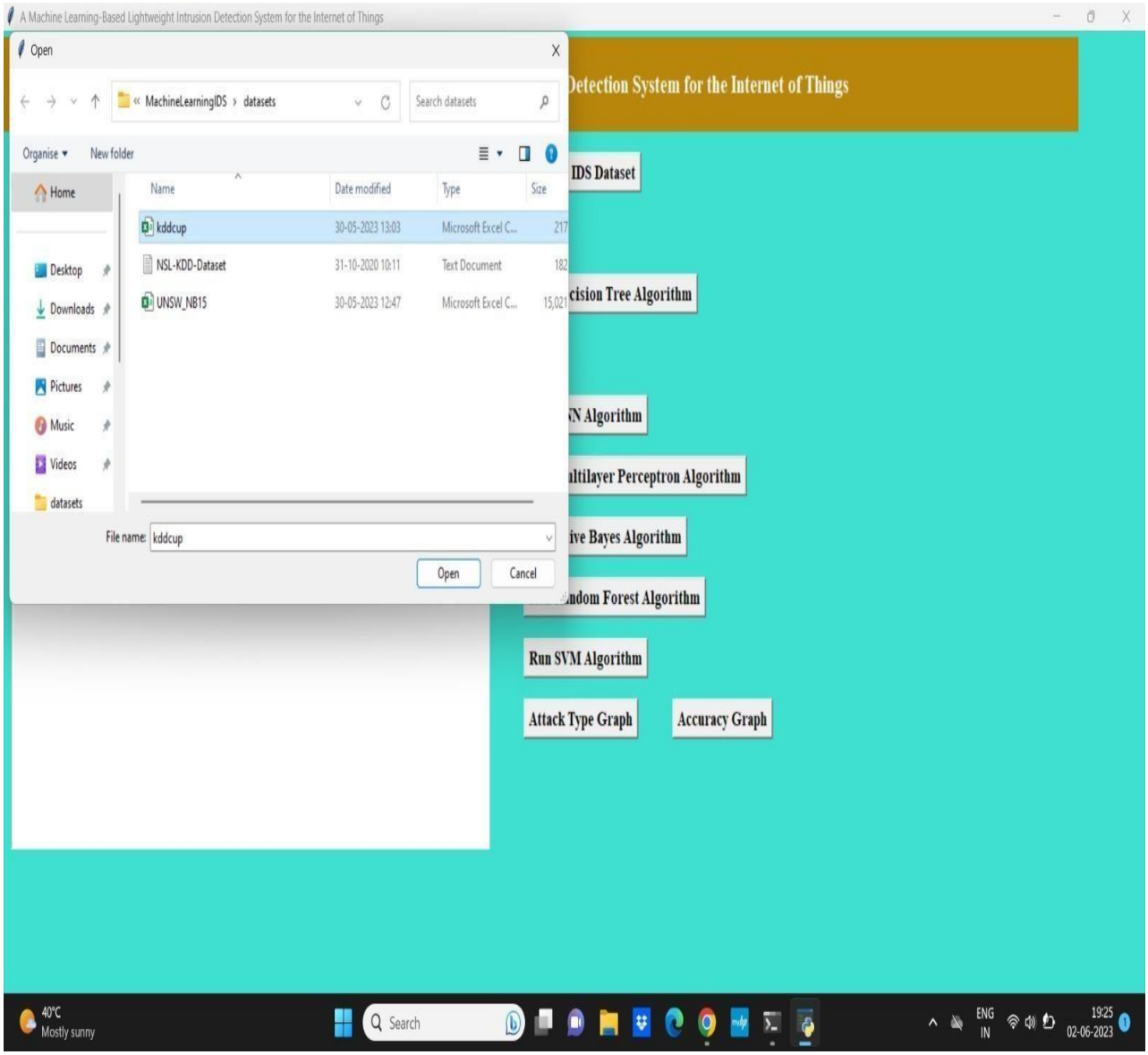

Fig 2: Selecting, Uploading ‘kddcup.csv’ dataset

In above screen selecting and uploading ‘kddcup.csv’ dataset and click on ‘Open’ button to load dataset and then application will perform dataset pre-processing and then apply feature selection algorithm and then split dataset into train and test part.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

Fig 3: Displaying various attacks

In above screen application displaying various attacks size available in dataset and then displaying total features and then displaying selected features and then displaying names of all selected features and then displaying total dataset size and total records used for training and testing. Now both train and test dataready and now run all algorithms by clicking on each button and then calculate accuracy, precision, recall and F-Score on test data.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

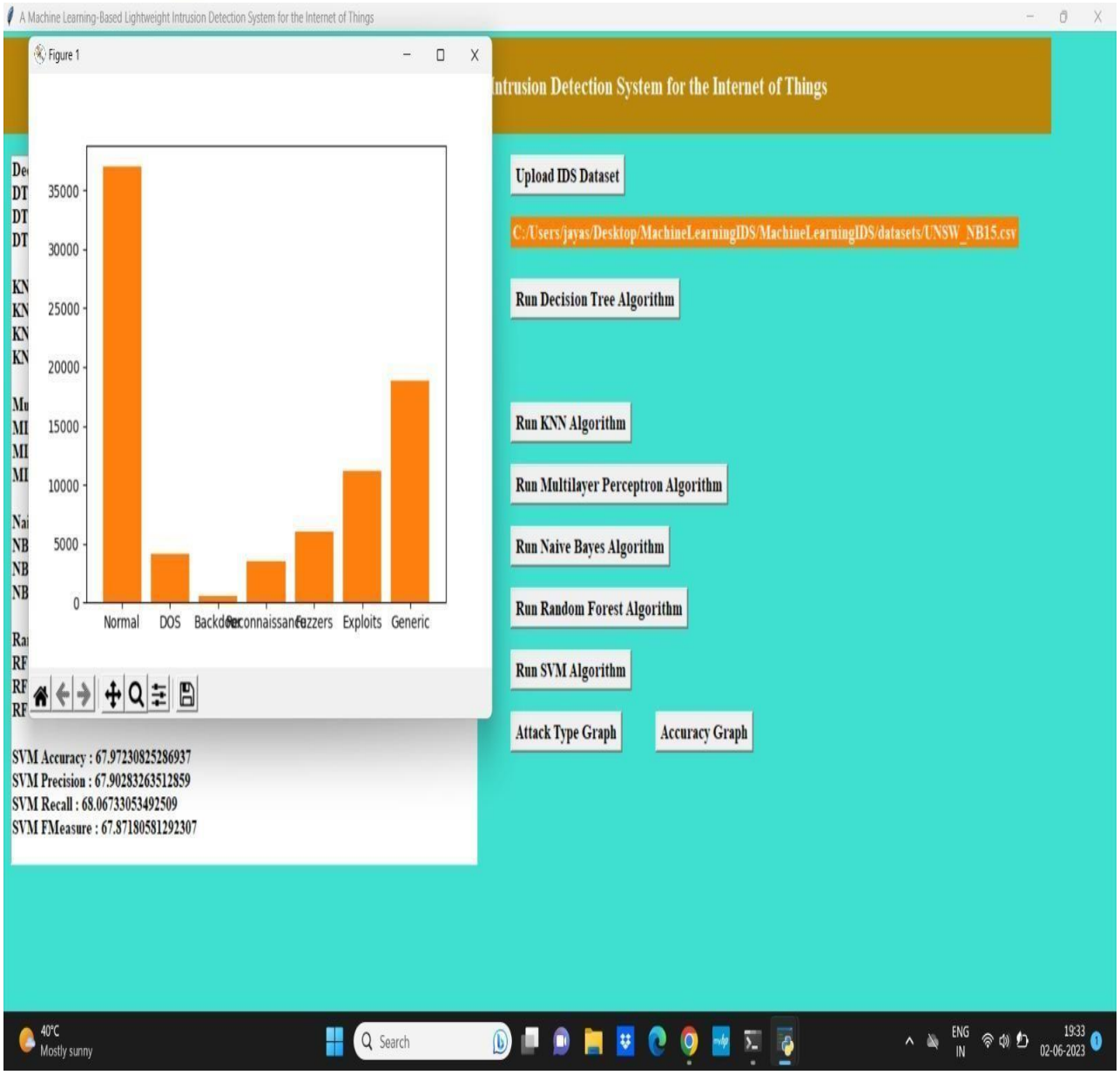

Fig 4: Attack Type Graph

In above graph x-axis represents attack name and y-axis represents count of each attack and now click on‘Accuracy Graph’ button to get below accuracy graph

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

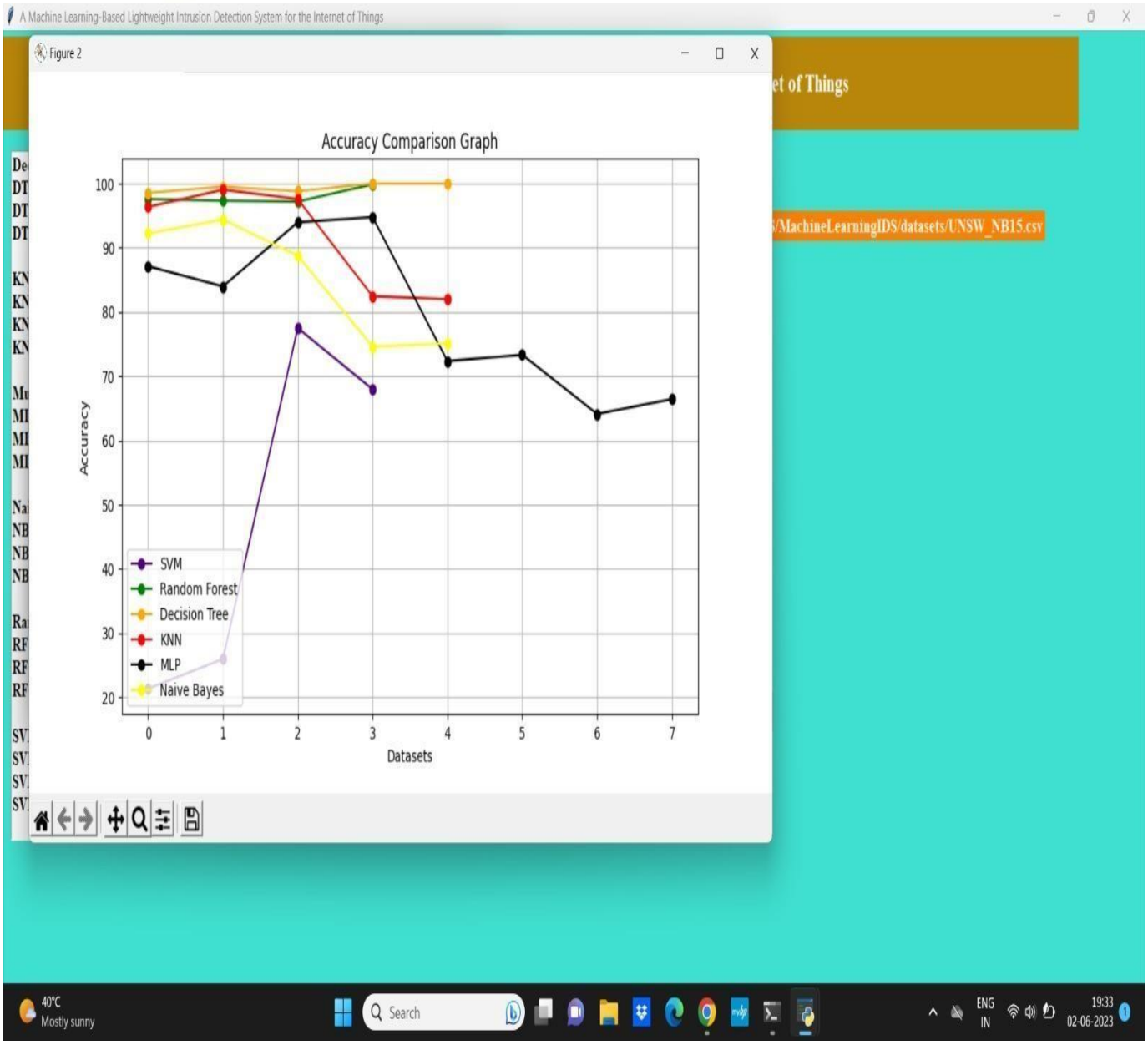

Fig 5: Accuracy Graph

In above graph x-axis represents 3 datasets and y-axis represents accuracy of each algorithm for that dataset.From all algorithms we can decision tree is giving good performance.

5.CONCLUSION

A lightweight intrusion detection model for Internet of Things (IoT) devices using machine learning techniques. The goal is to address the security challenges faced by IoT systems and provide protection against both internal and external attacks.

The authors evaluated several machine learning classifier models and applied three lightweight feature selection algorithms to find the best classifier models. The objective was to achieve a high accuracy and precision, as well as a low false negative rate. The experiments were conducted using the KDD99,NSL-KDD and UNSW-NB15 datasets for learning and evaluating the model.

According to the study's results, it was observed that decision tree (DT) and K-nearest neighbours (KNN)performed better than the other algorithms. However, it was noted that KNN took more time for classification compared to the DT algorithm. Additionally, the study utilized three correlation methods (PCC, SCC and KTC) to reduce the dimension of the datasets. The classifiers showed good performance when the correlation coefficient threshold was set above 0.9. Below this threshold, the performance was poor and sometimes unacceptable.

In terms of dataset performance, the NSL-KDD dataset yielded better results compared to the KDD99 and UNSW-NB15 datasets, including that the model performed well within the scope of the study area.

Overall, the proposed lightweight intrusion detection model based on machine learning techniques aimed to enhance security in IoT systems. The study evaluated various classifiers, applied feature selection algorithms and utilized different datasets to assess the model's performance and effectiveness

FUTURE SCOPE

In Future Work we will find out about different characteristic resolution techniques blended with extra laptop getting to know algorithms utilized to real-time statistics from IoT devices.

REFERENCES

[1]Atzori, L., Iera, A., Morabito, G. (2010). The Internet ofThings: A survey. Computer Network, 54(15): 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2]Weiser, M. (1991). The computer for the 21st century.Scientific American, 265(3): 94-105.

[3]Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016).Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology.IEEE ICC - Mobile and Wireless NetworkingSymposium. https://doi.org/10.1109/ICC.2016.7510811

[4]Raza, S.,Wallgren, L., Voigt, T. (2013). SVELTE: Real-time intrusion detection in the Internet of Things. Ad HocNetworks, 11(8): 2661-2674.https://doi.org/10.1016/j.adhoc.2013.04.014

[5]Anand, A., Patel, B. (2012). An overview on intrusiondetection system and types of attacks it can detectconsidering different protocols. International Journal ofAdvanced Research in Computer Science and SoftwareEngineering, 2(8): 94-98.

[6]Rajasegarar, S., Leckie, C., Palaniswami M. (2008).Anomaly detection in wireless sensor networks. IEEEWireless Communications, 15(4): 34-40.https://doi.org/10.1109/MWC.2008.4599219

[7]Li, W.C., Yi, P., Wu, Y., Pan, L., Li, J.H. (2014). A newintrusion detection system based on KNN classificationalgorithm in wireless sensor network. Journal ofElectrical and Computer Engineering, 2014: 8 pages.http://dx.doi.org/10.1155/2014/240217

[8]Thanigaivelan, N.K., Nigussie, E., Kanth, R.K., Virtanen,S., Isoaho, J. (2016). Distributed internal anomalydetection system for Internet-of-Things. 13th IEEEAnnual Consumer

Communications & NetworkingConference (CCNC).https://doi.org/10.1109/CCNC.2016.7444797

[9]Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultra-lightweight deep packet anomaly detection for Internet ofThings devices. 2015 IEEE 34th InternationalPerformance Computing and CommunicationsConference (IPCCC).https://doi.org/10.1109/PCCC.2015.7410342

[10]Huang, S.H. (2003). Dimensionality reduction inautomatic knowledge acquisition: A simple greedysearch approach. IEEE Transactions on Knowledge andData Engineering, 15(6): 1364-1373.https://doi.org/10.1109/TKDE.2003.1245278

AUTHOR PROFILES

Ms.M.ANITHA completed her Master of Computer Applications and Masters of Technology. Currently working as an Assistant professor in the Department of Masters of Computer Applications in the SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr. CH. SATYANARYANA REDDY Completed his Bachelor of Computer Applications at Acharya Nagarjuna University. He completed his Master Computer Applications at Acharya Nagarjuna University. Currently working as an Assistant professor in the Department of Computer Applications SRK Institute of Technology, Enikepadu, Vijayawada, NTR(DT). His areas of interest include Networks, Machine Learning & Artificial Intelligence.

Ms. P.JAYASRI is an MCA student in the Department of Computer Applications at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She has a Completed Degree in B.Sc.(computers) from Nalanda Degree College Vijayawada. Her areas of interest are DBMS, Java Script, and Machine Learning with Python.