IOT NETWORK ATTACK SEVERITY CLASSIFICATION

Bhukya Madhu[1*], Sanjib Kumar Nayak[2,], Veerender Aerranagula[3], E. Srinath[4], Mamidi Kiran Kumar[5] and Jitendra Kumar Gupta[6]

[1]Department of CSE- Data Science, KG Reddy College of Engineering & Technology, Telangana, India

[2,3] Department of Computer Science & Engineering, CMR Technical Campus(A), Hyderabad, India

[4]Department of Computer Science and Engineering, Keshav Memorial Institute of Technology (A), Hyderabad, India

[5]Associate Professor, Department of CSBS, GRIET, Bachupally, Hyderabad, Telangana

[6]Uttaranchal Instiiute of Technology, Uttaranchal University, Dehradun, 248007

Abstract. Lack of network security is a major roadblock for Internet of Things (IoT) implementations. New attacks have emerged in recent times, taking advantage of vulnerabilities in IoT gadgets. The sheer scale of the IoT will also make standard network attacks more potent. Machine learning has found a lot of use in traffic classification and intrusion detection. We present a methodology in this piece that can be used to spot fraudulent communications and determine the identity of IoT devices. To determine the origin of the generated traffic, the nature of the traffic, and the presence of network hazards, this framework collects features per network flow. To achieve this, it relocates the network's brains to its periphery. In order to discover which of several Machine Learning algorithms is superior to random forest, a number of them are pitted against one another. Using these Machine Learning methods, attacks can be ranked in terms of their potential damage. After running the tests, it was determined that TABNET has the highest accuracy (94.62%) for categorizing the network severity (93.51%) and that CNN has the lowest accuracy (93.51%) of the two.

Keywords— IoT, attack severity, network security, machine learning, and classification.

*Corresponding author: madhu0525@gmail.com

1 INTRODUCTION

There has been a lot of focus on the Internet of Things (IoT) and the characteristics it exhibits in published research. The recent change in the standards and restrictions imposed on security is what has drawn attention. In addition to introducing new security vulnerabilities on its own, the Internet of Things also offers a very robust platform from which attacks can be launched. The heterogeneity of linked devices, limitations on power and processing resources, and scalability are just a few of the traits that make the Internet of Things so infamous. These qualities are precisely what give rise to a number of security worries. All of these factors together make the security of the Internet of Things a unique and difficult issue. Identification of IoT devices is essential in this scenario in order to implement security controls and distinguish between different quality-of-service (QoS) levels. The issue arises from the lack of a single confirmed identification in this heterogeneous network, where the majority of identifiers (MAC addresses, IP addresses, Bluetooth ID, Zigbee ID, and so on) are susceptible to forging. The alternative is to make an effort to recognise IoT devices using characteristics that demonstrate these devices' behaviour.

Machine learning-based algorithms have been created for traffic classification and the detection of abnormal traffic patterns [84]. With the development of the Internet of Things (IoT), a new area of study that focuses on identifying objects based on the traffic they produce has developed in this environment. If the devices that generated the traffic can be identified along with the sort of traffic they produced, aberrant traffic can be detected. By establishing a match between the kind of device and the traffic generated at the network's edge, this objective can be achieved.

2 PREDICTION OF ATTACK TYPE

IoT (Internet of things) has low-power sensing devices in its network it has got various modes of communication, it can communicate with cloud, wired as well as wireless connections. As IoT devices are vulnerable, the hackers tend to attack these devices when compared with traditional computers and these attacks have subsequently increased in recent times. The reason for attacks is the lack of security options built in the system and also because the devices are outdated, also having weak login credentials is also the reason for increasing attacks.

The Proposed solution includes Machine Learning algorithms that are run on the user's computers, the malware detection is done based on patterns of network traffic. The patterns from the historical data can be stored in the database which can help in identifying the type of malware and this database can also be updated as required

The solution specifically targets bots that scan for and infect susceptible devices. It will take a very long time of the scanning and propagate the life cycle of a botnet, sometimes it may take from a few weeks to a few months. If previously any Distributed Denial of Service attack has taken place by using botnet and isolate the real-world attack can easily be identified, it is not difficult to detect the attack, and there are existing methods to protect against such attacks in the industry and the relevant literature. Network operators can take suitable counter measures when IoT bots are identified on their networks. These countermeasures include prohibiting IoT bot traffic and notifying local network authorities. The following are the paper's significant contributions:

- The majority of existing malware into different categories, as to make it easier to spot comparable malware and develop detection algorithms for it.
- Using test bed tests and packet capture utilities, evaluating the patterns of the network traffic to identify IoT malware from each category is done.
- Using machine learning techniques and the given traffic patterns, a modular system for detecting IoT malware activities is proposed.

2.1 Objective

The Internet of Things connects to existing networks at all times and in all locations, making it a pervasive technology. Because these devices have resource limitations to identify malware, the networks have to be built more intelligently to identify attacks. Malicious actors, on the other hand, implant botnet, causing terabytes of data to the network which eventually brings it down. The learning from previous attacks and implementing tactics lays the way for Machine Learning predictive models to be proposed to detect such attacks. When found, the Random Forest model proposed by this project can identify almost all malicious traffic.

In order to feed a dataset to an algorithm, in this case a model, machine learning, a branch of artificial intelligence, identifies hidden patterns that may aid in making predictions using past data. Very little research has been done on IDS using machine learning on IoT networks. The defense Advanced Research Projects Agency (DARPA) offered machine learning datasets that were used in recent research to test various models. Support vector machine (SVM), random forest (RF), naive bayes (NB), and multi-layer Deep Learning techniques were among the models used. The findings of this inquiry were beneficial, with RF being one of the top models. The conclusions were reported in terms of root mean squared error, mean absolute percentage error, receiver operating characteristic curve, and accuracy.

Nevertheless, there are two important restrictions to be placed on this study: The multi-class testing did not make use of the available datasets. In addition, the Bot-IoT dataset was incorporated into the research, and the models KNN, RF, adaptive boosting, TabNet, CNN, and NB were used to analyze the data. Excellent results were obtained from the study in terms of accuracy, precision, F1 score, and the total amount of time spent. This research uses a current dataset as well as a range of machine learning algorithms. However, none of the models were subjected to multi-class testing in this study. The authors employed different machine learning approaches for multi-class categorization.

Using a smart home dataset, this study compares several machine learning algorithms such as decision tree (DT), RF, SVM, and GNB. The study concluded that the optimum model for multiple class classification RF. This study demonstrates that high-quality results can be achieved using multi-class categorization. Additional algorithm testing could assist support the research's findings. Proposed approach for severity classification and attack type classification is shown in figure1

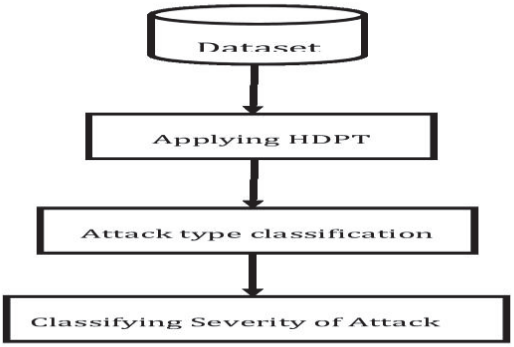

Fig 1: Overall approach for Attack type and severity classification

3 FEATURES DESCRIPTION

In all datasets, there was a class imbalance. For model training and testing, all of the regular traffic was mixed with an equal proportion of malicious traffic taken from the Maria and Baseline data sets [29]. Finally, observations were jumbled to avoid any trends. No specific target label defining the type of traffic exists. As a result, the dataset by identifying the normal and infected values is used. In addition to selecting features for each device, it was decided to build classes for each one and store important findings for easy access in the future. For each device in the data-prep directory, the class was likewise pickled. If a pickle file for a device has not yet been produced, it will run all models for that device before picking it.

Model Selection and Development

Supervised Learning methods was used to train and test the data for predicting malware attacks and used classification models including Logistic Regression.KNN Classifier, Decision Tree, XG Boost, and Random Forest, TabNet, CNN models, because the data was in multiclass classification.

"Recall" and "Accuracy" are chosen as measures to compare the performance of each model. Because it was intended to reduce the amount of (FN) False Negatives, which directly affect the data infected by malware in the wrong class, the most crucial metric is recalled. The accuracy of a model indicates its overall performance. Confusion Matrix is built for every device for testing and validation which falls under the visualization part while training the model.

Internet of Things as Interconnections of Threats

The most important issues at that time will be privacy and security. Various academic and industrial groups have diverse perspectives on the Internet of Things, but regardless of point of view [21], the IoT is still in its infancy and is vulnerable to several threats and attacks. The IoT cannot use the traditional networks or the Internet's prevention or recovery techniques due to its interconnection [1].

Attacks as Per Architecture

External attack: Security issues must be addressed first to fully utilize the benefits of the IoT [19]. The main worry is the cloud service provider's trustworthiness [17]. To gain the services, organizations purposefully dump both sensitive and non-sensitive data. However, they have no idea where their data will be handled or store

Wormhole attack: In ad hoc networks, the wormhole attack is fairly common. IoT connects both static and dynamic things, such as watches and refrigerators, as well as cars.

Selective forward attack: In other words, malicious nodes pick certain packets and then throw them away; this means that the filtration is done in a very selective manner, to allow the data packets to flow through. Some of the dropped packets may include sensitive data that has to be processed [21].

Sinkhole attack: Sinkhole attacks are most common on sensors that stay in the networks for a very long period of being unidentified. The hacked node gathers data from all the nodes around it. The result of this kind of attack will give chance to similar kinds of attacks eg fabrication, selective forward, etc.

Sewage pool attack: The goal of a sewage pool attack is for a bad user to attract all communications from a specific region to it; this will help lessen the intensity of the attack thereby swapping the base station nodes.

Witch Attack: When a legitimate node fails, the malicious node takes advantage of the situation. After the failure of the genuine node[21], any subsequent communication via the factual link will be directed through the malicious node, which will result in the loss of data.

Hello flood attack: During the attack of the hello flood, each of the items will present itself to all its reachable neighbours with a "hello" message. These neighbours can be found in the HELLO message tree. When a rogue node is present, it will cover a wide frequency band, as a result, it will be connected to all of the other nodes in the network, giving it the status of a neighbour.

Addressing All the Things in IoT: Virtual Machines IP is spoofed as a part of an attack which is another security issue for the server. Malicious people gain the VMs' IP addresses and install malicious computers on them to attack the users. As a result, attackers can gain access to users' personal information and utilize it for nefarious reasons.

DDoS (Distributed Denial of Server): At the beginning of a Distributed Denial of Service Attack, unwanted traffic is flooded with huge packets to capture and deplete memory resources. This is the first step in a DDoS attack [17], which can be carried out by hundreds or even thousands of attackers. During this time, legitimate requests are being prevented from reaching the DC, and the bandwidth that is available to the DC is being consumed.

Flash Crowd: On the Internet, the term "flash crowd" refers to both websites as well as the occurrence of any event that causes a big flow of people to reach that web page or website, the sudden increase in overall network traffic to a particular web page or the jump in traffic can happen for several reasons[20].

IP Spoof Attack: An impersonation attack, also known as spoofing, is a form of cyber attack in which the perpetrator assumes the identity of another individual to obtain unauthorized access to restricted resources or to steal information to accomplish these goals. This kind of assault can manifest itself in a wide variety of guises; for instance [19], an adversary can mimic a genuine user to get access to their accounts by spoofing the user's IP address. Spoofing an IP address is a sort of IP spoofing, which is a type of network attack.

Attack on Components

The Internet of Things connects "everything." These objects are diverse in character and communicate sensitive data across long distances. Data can be generated and manipulated by compromised sensors in addition to attenuation, theft, loss, breach, and disaster. Verification of the end-user is essential right off the bat; it's extremely important to differentiate between humans and machines at this stage. This fundamental discrimination is aided by several sorts of Completely Automated Public Turing tests to tell Computers and Humans Apart (CAPTCHA).

Connectivity Protocols-Based Attacks

IoT items use several connectivity protocols, which can be divided into wired and wireless protocols [21]. A wireless connection uses radio waves, whereas a wired connection

between IoT devices uses physical media. Communication systems' range, data speed, power consumption, spectrum usage, TCP/IP capabilities, and topology are crucial features [23].

Convolutional Neural Network

The CNN is a well-known deep learning architecture. Uses many representational layers in CNN. With the aid of nonlinear nonlinear transformations, approximation nonlinear functions, and this deep structure, CNN is able to automatically extract the representation characteristic from the raw data. A feature extractor made up of numerous convolutional layers is frequently followed by pooling layers and a softmax classifier in a traditional CNN system. The pooling layer decreases processing dimensions and speeds up processing while the convolutional layer gathers signal information. On its own, this design can achieve some regularisation. The acquired features are then classified using the top softmax layer.

Convolutional neural networks (CNNs) are utilised in voice and image applications where data is stored in feature sequences, as shown in Figure 2. CNN modelling is inappropriate for most tabular data since they do not presume a spatial relationship between attributes. To address this issue, the image generator for tabular data (IGTD) groups related features by allocating features to pixel coordinates. By reducing the difference between feature distance rankings and picture pixel distance rankings, the approach determines the optimal assignment. Compared to current transformation techniques, IGTD produces compact picture representations with superior feature neighbourhood structure preservation.

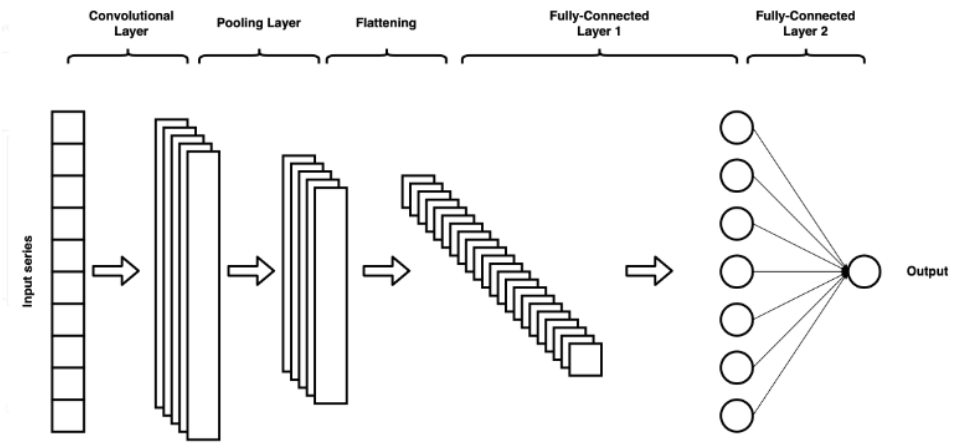

Fig 2: Convolutional Neural Network Architecture

TabNet

TabNet mimics decision trees with sequential attention [25]. In summary, it is a multi-step neural network with two critical actions each step (see figure 3):

- The attention transformer selects the most important features for processing in the next step
- Use feature transformer to process features into more useful representations

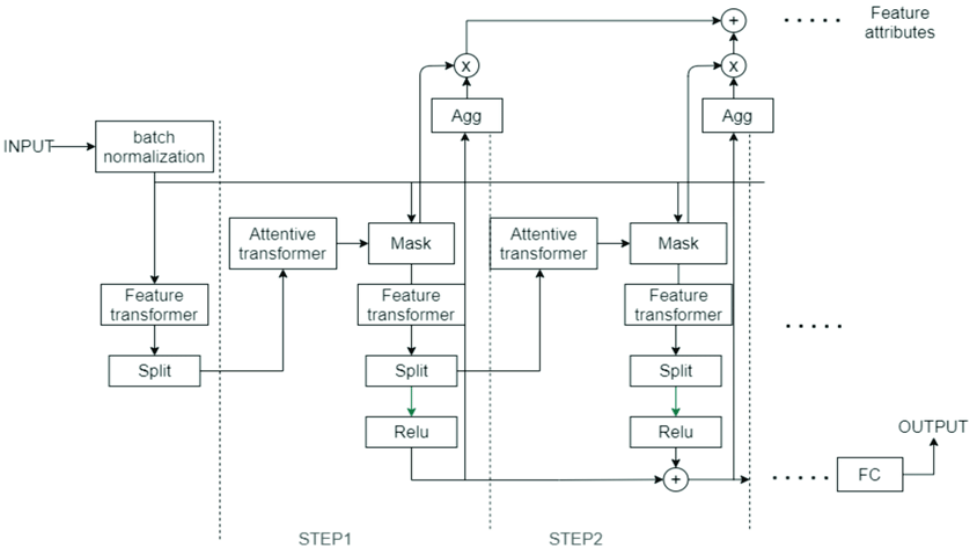

Fig 3: TabNet Architecture

Finally, the model uses the output of feature transformer for prediction later. Tabnet uses both attention and feature transformers to simulate the decision-making process of tree based model [25]. For example, the following prediction of adult census income data set, the model can select and process the most useful features for the task at hand, so as to improve interpretability and learning ability.

$$\mathbf{M[i] = Sparsemax(P[i-1] * hi(a[i-1]))}$$

Put them together, the main idea of tabnet is to apply feature and attentive transformers components in order, so that the model can simulate the generation process of decision tree. The attentive transformer performs feature selection, while the feature transformer performs transformations that allow the model to learn complex patterns in the data. You can see a chart below that summarizes the data flow of the 2-step tabnet model.

First, the initial input feature is transferred through the feature transformer to obtain the initial feature representation. The output of this feature transformer will be used as the input of the attention transformer. The attention transformer selects a feature subset and passes it to the next step. There will be a super parameter to set the number of times to repeat this step.

The model generates the final prediction by using the feature transformer output of each decision step. In addition, at each step, pay attention to the mask to understand which features are used for prediction. These masks can be used to obtain local feature importance and global importance.

TabNet chooses which model characteristics to draw on at each stage of the model using a machine learning method known as sequential attention. This method enables the model's predictions to be explained and aids in the model's ability to develop more precise models.

Experimental Results

Table 1: Overall accuracy of the test set classifiers

	Accuracy	F1_Score	Recall_Score	Precision_Score
SVM	0.73	0.77	0.75	0.77
RF	0.87	0.87	0.86	0.86
GNB	0.62	0.63	0.64	0.64
CNN	0.94	0.94	0.93	0.94
DT	0.85	0.83	0.83	0.83
KNN	0.75	0.75	0.75	0.76
TabNet	**0.96**	**0.95**	**0.92**	**0.95**

By looking at the results, it can be concluded that TabNet is the best performing Deep learning algorithm with the accuracy of 96 percent, CNN is the second-best among all the algorithms with an accuracy of 94 percent, and GNB is the worst performing machine learning algorithm with 62 percent accuracy. Table 1 is the details analysis of all the machine learning algorithms used in the objective. Various parameters like Accuracy, Precision-Recall, and F1 Score are discussed.

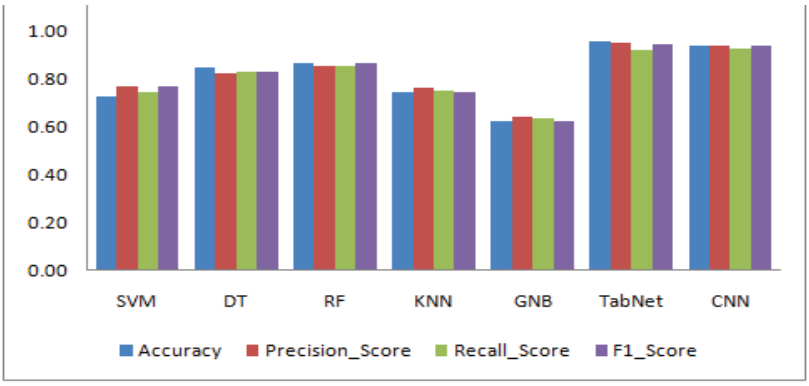

Fig 4: Comparative analysis of performance of Attack type and severity classification

Attack Severity Detection

Although the IoT's characteristics and security restrictions have undergone extensive study, it also offers a robust platform for cyber attacks. IoT is prone to security issues because of its widespread use, diversity of connected devices, power, processing capacity, and scalability. Each of them makes IoT security difficult to implement and complex. Security and QoS need the identification of IoT devices. Without a specific authorised identification, it is challenging to operate in this heterogeneous network (e.g., Zigbee ID, IP addresses, MAC addresses, Bluetooth ID, etc.). Internet of Things devices can be located by looking for behavioural characteristics. More than 66% of small firms have experienced a cyber

attack in the last year, the majority of which are targeted, according to research on small business data used to understand network attacks [14] and the need to use machine learning to thwart them. Attacks on device security, including phishing, rose by 33%, and attempts to steal credentials, by 30% [17]. These attacks will have a range of consequences, such as losses in reputation, money, and productivity.

Systems using machine learning categorise traffic [24] and find unusual traffic patterns. This led to a change in research focus. Devices and their traffic can be identified, but five machine learning and two deep learning methods (SVM, Decision Tree, Random Forest, KNN, GNB, TabNet, and CNN) were used to assess the severity of faults.

Following a comparison of various algorithms, it was discovered that TabNet has a 95% accuracy rate, whereas GNB has a 58% accuracy rate.

Network traffic is influenced by the operating system, installed apps, memory size [1], network protocols, and CPU power of the device. Consequently, it is possible to distinguish between attacks on standard IoT devices. Numerous intrusion detection systems (IDSs) based on machine learning streamline and automate detection [21, 25]. IoT networks require a scalable management solution because it takes time to add traffic control features to an existing network.

Statistic Dataset

Telstra, a telecom business that provides mobile, internet, and TV services, provided the data. This tabular data contains tonnes of network and disturbance data. examine data and predict severity using various features.

- train.csv—training set for fault severity
- Test.csv—set of tests for fault severity
- Sample_submission.csv demonstrates the appropriate input format.
- main dataset event type: event_type.csv • log_feature.csv: extracted log file features
- severity_type.csv: severity of log warnings • main dataset resource type: resource_type.csv

The following CSV files were utilised in this example: event type.csv, log feature.csv, resource type.csv, severity type.csv, and target class variable.csv. There are three severity levels for network issues: 0, 1, and 2. "Fault severity" is the goal variable used to gauge faults that network users have reported. Except for train.csv, test.csv, and sample submission.csv, all CSV files have been combined into one primary key-based CSV file.

Table 2: Data Set Overview

id	location	Fault severity	severity_type	event_type	resource_type	log_ feature	Volume
14121	location 118	1	severity_type 2	event_type 34	resource_type 2	feature 312	19
9320	location 91	0	severity_type 2	event_type 34	resource_type 2	feature 315	200
14394	location 152	1	severity_type 2	event_type 35	resource_type 2	feature 221	1
8218	location 931	1	severity_type 1	event_type 15	resource_type 8	feature 80	9
14804	location 120	0	severity_type 1	event_type 34	resource_type 2	feature 134	1

This analysis uses network disruption data to detect disturbances by location, fault severity, event kind, etc. For this data set, various datasets on network disruption were merged into one file, checked for missing values, and cleaned before analysis. Table 2 shows the first five rows of data using the python function head and the data set's size (73, 81, 19).

Visual Analysis

Fig 5: Heat Map

The figure 5 shows the heat map based on location and fault severity, volume looking at the graph it can be inferred that the highest volume 1.0.

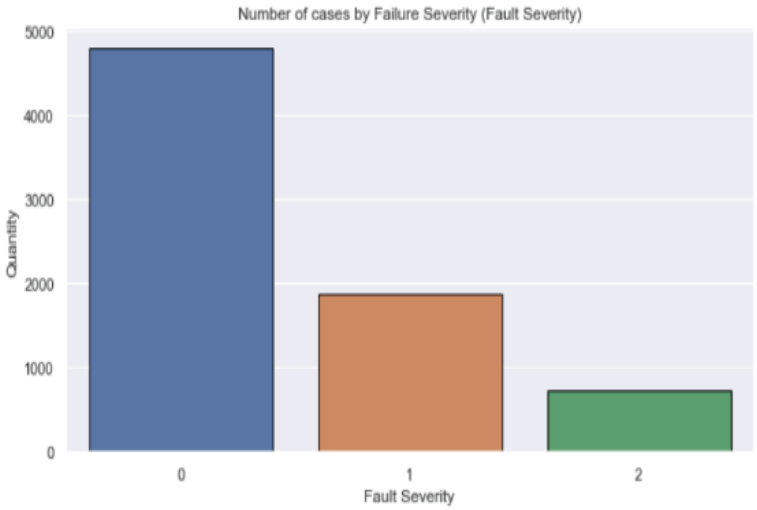

Fig 6: Severity Type Cases

The distribution of fault severity counts according to their various classes (0, 1, and 2) is shown in Figure 6. From the graph, it can be inferred that the majority of defects, or just under 5000, belong to class 0, the second-highest, or just under 2000, belong to class 1, and the lowest, or just under 1000, belong to class 2

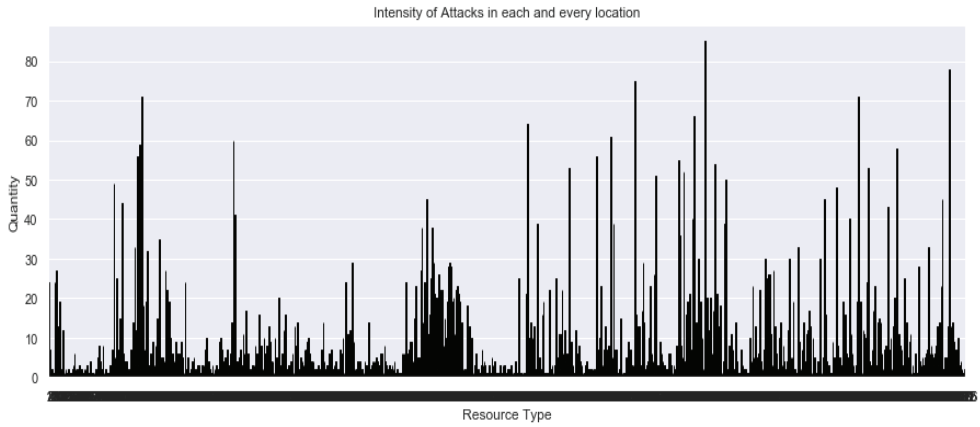

Fig 7: Location-based assault intensity

Figure 7 illustrates the plotting of assault intensity according to location and resource type. From the graph, it can be deduced that the bulk of attack intensities fall between 0 and 30, with the maximum intensity being about 85.

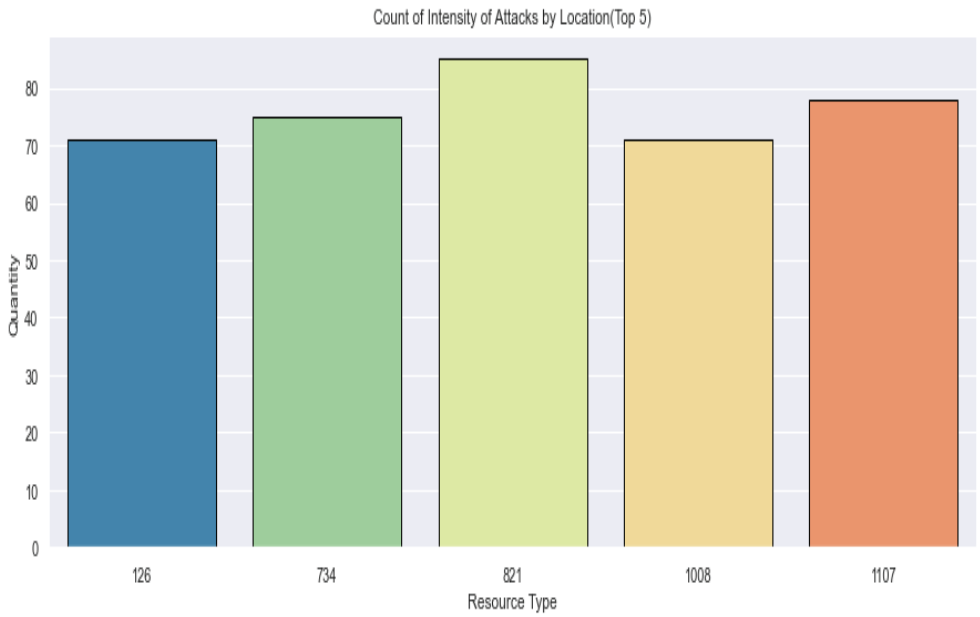

Fig 8: Resource types can be counted as a measure of the attack's potency

According to the figure 8 bar graph, the top 5 attack intensities according to location and resource type are plotted. The greatest intensity is about 85, and the top 5 places with the most attacks are 821, 1107, 734, 126, and 1008 accordingly.

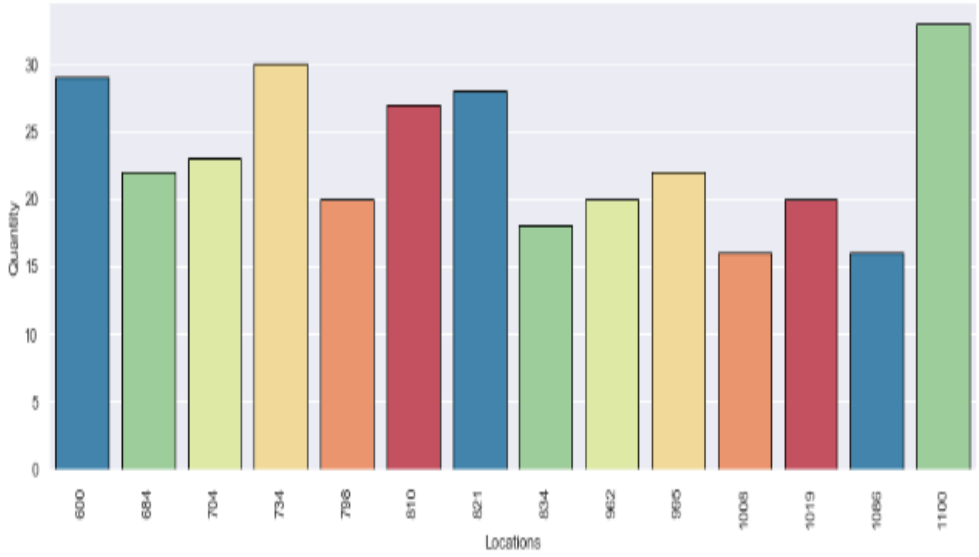

Fig 9: Location-based assault intensity counts

Data on network disruptions offers some excellent information. Figure 9 of the plotted chart above displays 14 locations with class 1 faults. By examining the visualisation, it can be deduced that location 1100 has the most type one defects, with just over 30 in total. The chart plots location against the count of type 1 faults.

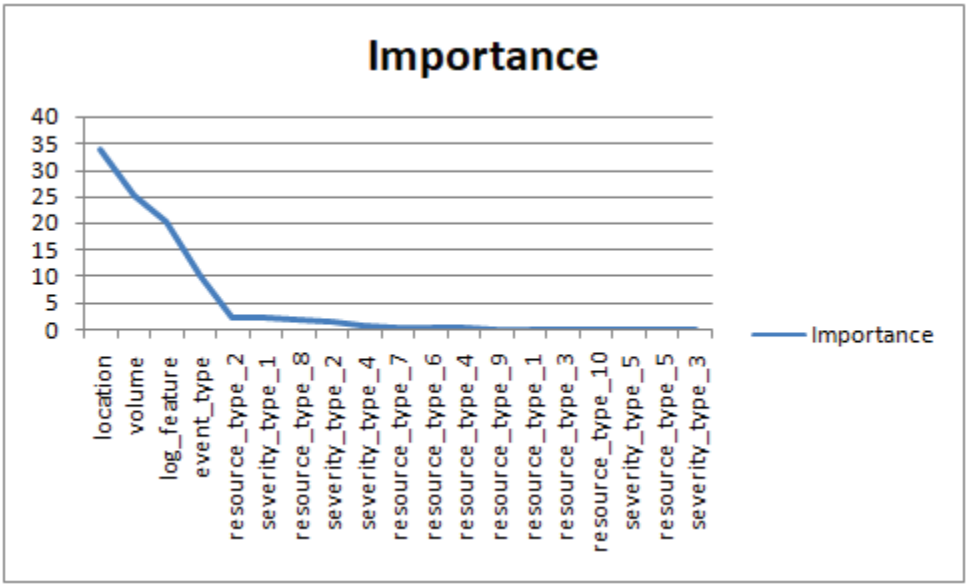

Fig 10: Features of a dataset based on their importance

IoT Network Disruptions are rarely studied due to a lack of publicly available datasets [15,27]. The experimental results show that network disruption data analysis can help protect IoT networks. the primary factors contributing to the depicted in figure 10 models—location, volume, log_feature, and evet_type—contribute 90%, while the rest contribute 10%.

Identifying network disruptions by location and categorising them by fault severity will help identify irregularities in the network and their causes, helping users increase safety measures. To do this, various ML algorithms were compared, and these comparisons provide very good insights into the performance of each model based on various parameters like accuracy, precision, and speed.

CONCLUSION

The project's main objective is classifying attacks. The project details ML methods. First extracted data this way. To classify and identify the assault type, the dataset is cleaned and pre-processed to the machine's scale. Finally, feature engineering selects traits to accurately classify and detect attack kinds. This strategy completely utilised machine learning. It removed the complex processes of manually extracting features and shortened the intelligent algorithm's training time and labelled data needed to accurately classify and identify items.

The Internet of Things can revolutionise global challenges by giving humans power. The IoT could revolutionise the world. IoT smart services let network users access, link, and store data from anywhere. The Internet of Things (IoT) may simplify, speed up, and connect us to the virtual world via smart devices, but its safety is a major concern.

IoT smart services let network users access, link, and store data from anywhere. The Internet of Things (IoT) may simplify, speed up, and connect us to the virtual world via smart devices, but its safety is a major concern. This project provides a systematic literature study of Machine Learning-based IoT security, including an overview of the Internet of Things and its architecture, a thorough examination of various security threats, ML-based algorithms, security solutions, and future challenges that can help the research move forward.

Over the past few years, the IoT paradigm has unleashed a wide range of dangers to the safety and privacy of IoT devices and humans. These risks will prevent this paradigm from being implemented. Despite a record number of security breaches in the Internet of Things (IoT) sector, there is no common way to detect or respond to them. This work attempts to classify IoT attacks using a novel building-blocked reference model and provide mitigation methods. Implementing all of these security controls and procedures at once requires device compute and battery power, which is incompatible with IoT technology and its components. A lightweight, sturdy security system that can handle the most serious security threats is needed for IoT technology. Many IoT attacks have been classified. By confirming node identification during transmission or using hard-to-tamper hardware, application developers can prevent some of these dangers.

Classifying and diagnosing unknown network interruptions using ML algorithms is the paper's main goal. First retrieved interrupted network traffic data. Then the dataset is cleaned and pre-processed to make it machine-readable, and all the files are merged into one file to help us classify and identify fault severity. Finally, feature engineering automatically selects feature vectors to classify and discover unknown network disruptions quickly and efficiently. This strategy completely utilised machine learning. It eliminated the complicated steps of manually extracting features and reduced the intelligent algorithm's training time and labelled data requirements by ensuring classification and identification accuracy.

REFERENCES

1. Singh and B. Sikdar, "Adversarial Attack and Defence Strategies for Deep-Learning-Based IoT Device Classification Techniques," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2602-2613, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3138541.
2. M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, vol. 22, no. 3, pp. 1646-1685, 2020, doi: 10.1109/COMST.2020.2988293.
3. Q. Zhang, J. -H. Cho, T. J. Moore and I. -R. Chen, "Vulnerability-Aware Resilient Networks: Software Diversity-Based Network Adaptation," in IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3154-3169, Sept. 2021, doi: 10.1109/TNSM.2020.3047649.
4. H. Xu, W. Yu, D. Griffith and N. Golmie, "A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective," in IEEE Access, vol. 6, pp. 78238-78259, 2018, doi: 10.1109/ACCESS.2018.2884906.
5. C. Garrido-Hidalgo, D. Hortelano, L. Roda-Sanchez, T. Olivares, M. C. Ruiz and V. Lopez, "IoT Heterogeneous Mesh Network Deployment for Human-in-the-Loop Challenges Towards a Social and Sustainable Industry 4.0," in IEEE Access, vol. 6, pp. 28417-28437, 2018, doi: 10.1109/ACCESS.2018.2836677.
6. O. B. Mora-Sánchez, E. López-Neri, E. J. Cedillo-Elias, E. Aceves-Martínez and V. M. Larios, "Validation of IoT Infrastructure for the Construction of Smart Cities Solutions on Living Lab Platform," in IEEE Transactions on Engineering Management, vol. 68, no. 3, pp. 899-908, June 2021, doi: 10.1109/TEM.2020.3002250.
7. Yin, Chuanlong, et al. "A deep learning approach for intrusion detection using recurrent neural networks." IEEE Access 5 (2017): 21954-21961.
8. P. Ferrari et al., "On the Use of LoRaWAN and Cloud Platforms for Diversification of Mobility-as-a-Service Infrastructure in Smart City Scenarios," in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-9, 2022, Art no. 5501109, doi: 10.1109/TIM.2022.3144736.
9. Lasi, Heiner, et al. "Industry 4.0." Business & information systems engineering 6.4 (2014).
10. M. Aazam, S. Zeadally and K. A. Harras, "Deploying Fog Computing in Industrial Internet of Things and Industry 4.0," in IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4674-4682, Oct. 2018, doi: 10.1109/TII.2018.2855198.
11. C. -C. Lin and J. -W. Yang, "Cost-Efficient Deployment of Fog Computing Systems at Logistics Centers in Industry 4.0," in IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4603-4611, Oct. 2018, doi: 10.1109/TII.2018.2827920.
12. Peralta, Goiuri, et al. "Fog computing based efficient IoT scheme for the Industry 4.0." 2017 IEEE international workshop of electronics, control, measurement, signals and their application to mechatronics (ECMSM). IEEE, 2017.

13. Kilkki, Kalevi, et al. "A disruption framework." Technological Forecasting and Social Change 129 (2018).
14. Sejdovic, Suad, and Natalja Kleiner. "Proactive and dynamic event-driven disruption management in the manufacturing domain." 2016 IEEE 14th International Conference on Industrial Informatics (INDIN). IEEE, 2016.
15. Modarresi, Amir, and James PG Sterbenz. "Toward resilient networks with fog computing", IEEE, 2017.
16. Sterbenz, James PG, et al. "Redundancy, diversity, and connectivity to achieve multilevel network resilience, survivability, and disruption tolerance invited paper", Telecommunication Systems 56.1 (2014).
17. Madhu Bhukya, et al. "Intrusion detection models for IOT networks via deep learning approaches." Measurement: Sensors 25 (2023): 100641.
18. J. P. Sterbenz, D. Hutchison, E. K. C¸ etinkaya, A. Jabbar, J. P. Rohrer,M. Scholler, and P. Smith, "Resilience and survivability in commu- ¨nication networks: Strategies, principles, and survey of disciplines,"Computer Networks, vol. 54, no. 8, pp. 1245–1265, 2010.
19. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internetof things for smart cities", IEEE Internet of Things Journal, vol. 1,pp. 22–32, Feb 2014.
20. D. Clark, K. Sollins, J. Wroclawski, D. Katabi, J. Kulik, X. Yang,R. Braden, T. Faber, A. Falk, V. Pingali, M. Handley, and N. Chiappa, "New arch: Future generation Internet architecture", technical report,DARPA, MIT, ISI, February 2003.
21. Madhu, Bhukya, and M. Venu Gopalachari. "Classification of the Severity of Attacks on Internet of Things Networks." Sentiment Analysis and Deep Learning: Proceedings of ICSADL 2022. Singapore: Springer Nature Singapore, 2023. 411-424.
22. Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE communications surveys & tutorials 17.4 (2015).
23. Reinike, William J. "The US Financial System as a Network: Insights and Implications for Hybrid Warfare", Naval Postgraduate School, 2020.
24. Feldman, Zohar, et al. "Proactive event processing in action: a case study on the proactive management of transport processes (industry article)", Proceedings of the 7th ACM international conference on Distributed event-based systems. 2013.
25. Metzger, Andreas, Rod Franklin, and Yagil Engel. "Predictive monitoring of heterogeneous service-oriented business networks: The transport and logistics case", 2012 Annual SRII Global Conference. IEEE, 2012.
26. Yan, Jianzhuo, et al. "Rainfall forecast model based on the tabnet model", Water 13.9 (2021).
27. Engel, Yagil, and Opher Etzion. "Towards proactive event-driven computing", Proceedings of the 5th ACM international conference on Distributed event-based system. 2011.
28. Kaluža, Boštjan, et al. "An agent-based approach to care in independent living", International joint conference on ambient intelligence. Springer, Berlin, Heidelberg, 2010.

29. Brzezinski, Jack R., and George J. Knafl. "Logistic regression modeling for context-based classification", Proceedings. Tenth International Workshop on Database and Expert Systems Applications. DEXA 99. IEEE, 1999.