**SPAM DETECTION IN IOT DEVICES**

**Rishitha.G1,Siri Chandana.M2**

**1.ABSTRACT:**

This review paper is all about detecting the spam in IoT devices using machine learning techniques. They help in identifying and segregating the irrevelent/unnecessary information. IoT helps in the building link between real-world problems. IoT has been grown rapidly more than 25 billion devices. These iot devices will produce data with different models that are having different quality of data. This consumes a lot of time to detect the spam in different effective ways. We can successfully detect the spam using different machine learning techniques. In this review paper we used different machine learning models. At present, there is a huge demand for security and safety so this detection of as spam will help many people. Machine learning algorithms ensure security and usability in IoT systems. Most of the hackers use these ML models/techniques in IoT devices in a negative way. To eliminate the generation of harmful input by IoT devices, a spam detection technique is proposed. This data is being divided into different no. of sets and then provides it to all the ML methods in the process. Here we used different ML models. The performance of each model is analyzed. We use this to detect the spam in IoT devices. Each model gives the spam accuracy.

**2.INTRODUCTION:**

Spam refers to unsolicited and unwanted messages, usually sent in bulk. There are different types of spam, like email spam, SMS spam, and even social media spam.They can contain unwanted advertisements, scams, or malicious links. It's best to be cautious and avoid engaging with spam messages.

In recent years, the proliferation of IoT-based devices has revolutionized various industries, bringing convenience and efficiency to our daily lives. However, along with the benefits, there are also challenges, such as the increasing threat of spam and malicious activities targeting these devices. Iot devices must ensure whether the data is secured and also need to check the privacy issues like hacking, jammers, spam, etc..[1] This review paper aims to explore the topic of spam detection for IoT-based devices

Mostly we use supervised machine learning methods [2], where the system is trained on labeled data. This training allows the model to identify key features and patterns associated with spam, enabling it to make informed decisions [3].

Another approach is unsupervised learning, where the system learns from unlabeled data to identify anomalies.[4] By detecting unusual patterns, the system can detect potential spam attacks and take appropriate actions to rectify them.

We have gone through a total of 50 different research papers written in recent times , In our knowledge with these research papers they have used different varieties of data models for training the given data set and to foresee the accuracy of spam detection using different models like Bayesian ,bagged ,support vector machine ,supervised, unsupervised learnings etc.,The most common approach is that they have used these models to assign F-score to each item which intern is used to predict the spam .

Stay tuned for more insights and findings as we navigate the world of spam detection in IoT-based devices

**3. LITERATURE REVIEW**

3.1 SUMMARY:

Hackers often learn algorithms to detect vulnerabilities in IoT based devices. In this project they used machine learning to detect spam to protect IoT devices. here every ML model will calculate the accuracy. This score helps in letting us know the honesty of each device in different situations. The accuracy is used to decide the reliability of each device in organizing the smart home. This produces what conditions are efficient ,secure operating of IOT devices .Throughout these years the devices that are available on online are increasing and similarly the quality of data given by the devices would have also increased. They have collected data from REFIT project. The data preprocessing makes special impact as the number of features are reduced. They have used PCA for feature reduction. This reduces the amount of variation between different characteristics . This resulted in a more defined set of requirements that need to be met before Internet of Things devices can function properly. They have used decision tree and svm to evaluate the spam score for IoT devices. In order to prevent the irrelevant information this research on detection in IoT devices was introduced. We took the help of several machine learning models in detecting the spam This helps to reduce the spam from the devices. They got an accuracy of 99.1% on test set by using these 2 models. smart devices are largely used on day to day lives. Different ML models, data mining techniques are used in this project for cyber analytics for spam detection. They have used support vector machine algorithm extracted the feature, CNN algorithm is used to extract color, shape, texture features. There are drawbacks in the existing systems like it is ineffective because of inefficiency of detection of spam in different IoT devices and it also has some merit/advantages i.e, here the spam detection is justified from various ML models. It computes accuracy of each mode and then used for detection. The spam score used to decide the usability of IoT devices in organizing the smart home. From now on, we also consider climatic changes the devices to make it more secure. Emails are basically divided into 2 categories they are spam and ham. Here several machine learning techniques and deep learning models like random forest, svm, etc. are being used in filtering the spam.

**3.2 Table: LITERATURE SURVEY**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| PAPER TITTLE | MODEL USED | | PARAMETERS USED | MERITS | | LIMITATIONS |
| Author:  Dr.D. Tejaswini  (2023) | . SVM  . RF  . Bayesian model  . naïve bayes  . boosting | | . Vars  . m stop  . nu  . n rounds  . lambda  . alpha | . spam score | | .Less performnace |
| AUTHOR:  @Aijaz Ali Khan all  (2021) | . (SVM)  . neural networks  . RT  . DT | | .Principal component analysis (pca) | . correlation between discrete attributes and continuous attributes | | . uncertainity |
| Author: ch. Drakshayani  (2020) | . RT  . SVM | | . Data collection  . data preparation  . model selection  Analyse  and prediction | . save energy | | .reduces efficiency |
| Author: Samira Dehghani  (2023) | . Recurret  neural networks  . Graded recurrent  Unit  .Bidirectionalrated recurrent  .Convolutional neural network  . NSGA II optimization with multiple objectives. | | . Long shor term memory | .model  loss is minimized | | . less FPR and f1-measure |
| Author:  D.Varalami  (2019) | . SVM  . RT  . naïve bayes | | . Kernal trick | .volume of data increases | | . use image data |
| Author:  S.Mounasri  (2023) | . Bagged model  . support vector machine  . extreame gradient model  . Generalized model | | . Bag  . bayes | . reliability | | . less effective. |
| Author:  Naeem Ahmed  (2018) | . SVM  . RF  . NN  . DT | | . accuracy  . precision  . recall  . F-score | . scalable and language independent | | . Cannot handle Url’s |
| Author:  Ameena Zainab  (2022) | . DT  . naïve bayes  . gradient boosting  . Extreme Gradient | | . Spamicity  . Maxdepth  . N\_estimators  . hyper-parameter tuning | . determine the spamicity score | | . not easy to define a threshold. |
| Author:  Aditya Tandon  (2022) | .Convolutional neural networks (CNN)  . deep learning models  . logistic regression  . RF | | . Data processing  . deep walk  . GCN | . precise and efficient. | | . low computational complexity |
| Author:  P.Akshitha  (2021) | . Boosted linear model  . support vector machines . KNN’s  . reinforcement  ML Techniques | | . Feature engineering feature selection  . PCA (principal component analysis) | . Detects the spam parameters. | | . The info is incorporative |
| Author:  Potbhare nitin Balasaheb  (2020) | . bayes model  . boosting  . extreme gradient model  . generalized model | | . Data gathering.  . data processing | . find the spam parameters | | . Position dependency speed of time |
| Author:  P.Raghu  (2020) | . (SVM)  . RF  . Spamicity Score  . Extreme Gradient  . Boosting (XGBOOST)  . DT | | . Networked heterogenous detectors  . light weight shielding technique | . calculate spamicity rating | | . strategies are absent |
| Author:  Dr.K.Srinivasa rao  (2020) | .SVM  . random forest  . K-nearest neighbours  . neural network model  . logistic regression | | . Recursive feature elimination  . PCA (principal component analysis) | . uses training data and feedback from humans | | . Maintains strategic distance from digital assaults. |
| Author:  K.Bhanu Naveen teja  (2018) | . LR  . SVM  . RF | | . preparation of data, model  . Selection  saving trained model | . Gives more accuracy | | . difficult to manually review. |
| Author:  Sarfaraj Alam  (2021) | . K-nearest neighbours  . reality mining algorithm,  . DBSCAN  . isolation forest | | .Cognitive spammer framework (CSF)heatmap  . Recursive feature elimination  . chi-square | . it will easily detect the anamoly before it enters into the iot device. | | . Corporation among smart entities |
| Author:  G.Uday kumar  (2019) | | . SVM  . RF  . DT | . Spamicity Score  . Extreme Gradient Boosting (XGBOOST) Algorithm | | . system gaining knowledge of fashions. | . less overall performance |
| Author:  Sidharth, Vasantha  (2018) | | . supervised learning  . Classification  . Regression  . unsupervised learning | . Data gathering.  . data processing | | . Dataset used are preprocessed by using feature enginerring. | . used im small range home appln |
| Author:Sriram.s(2021) | | . Pre-processing  . Deepconvolution neural network models | .Cost sensitive learning  . transfer learning  . Statistical metrics | | . accuracy  . precision  . FPR | . low performance |
| Author:  Heba  Mohammed laique  (2020) | | . Bagged Model  . Bayesian Generalized . Linear Model  . Voting Classifier  . Ada boost  . Decision tree  . sequential model  comparison graph | . Data preprocessing  . Feature selection | | .They have separate login | . Sequential model |
| Author:  Alanazi Rayan  (2018) | | . Random  Forest  . Decision tree | .correlation-oriented feature extraction (CFS) approach. | | .predict the accurate solution | . less efficient |
| Author:  L.K Adwani  (2020) | | . Bagged model,  . Bayesian generalized model  . Boosted linear model  .eXtreame  Gradient model  .Generalised | . Bstlm  . glm-stepAIC | | . uses web spam detection. | . technical problems |
| Author:  Nurussabah Mohammad Fahim  (2020) | | . Supervised  . unsupervised  . reinforcement  . Partially supervised  . Svm  . ramdom forest  . Boosting of extreme gradients (XGboost) | . Sklearn  . xgboost | | . uses 5 different aiml techniques | . less accuracy |
| Author:  DR.S.  Jayanthi  (2018) | | . Random forest algorithm. | . preprocessing of data  . training the model  .Model evaluation,  .Model Performance analysis | | .Accurate detection  . Customizable  .User-friendly interface | . Can be  improved |
| Author:  Sanket  (2018) | | . Supervised learning  . Classification  Regression  . Unsupervised learning | .Performance analysis | | .preprocessed dataset is used | . Less number of features in the dataset |
| Author:  Shravani.U  (2021) | | . Bagged model  . Bayesian model . | . Feature choice  .Entropy-based filter | | .preprocessed dataset is used. | . Same as other models |
| Author:  Anisha.P Rodrigues  (2020) | | .Backpropagation neural networks  . Naïve bayes  . support vector  . machine method  . sequential minimal  . optimisation algorithm | .Lexicon-based sentiment  analysis | | .it being directly experimented on real-time data/objects | . the size of the lexicon set is very small is it depends on the domain |
| Author:  Maryam Anwar  (2018) | | . DT  . SVM  . RF  . BOOSTING ADA | .Reinforment learning  . Accuracy | | .analyse different iot devices | .Complicated dataset |
| Author:  Mr.D Murahari Reddy  (2019) | | . SVM  . naïve bayes  . boosted linear model | . (PCA) | | . information has constant, multisource, rich, and meagre | . Prior information is incorporated |
| Author:  Ms.Pragathi Rana  (2019) | | . k-means,  . RNN  . K-N, naive bayes  .support vector machine | .Graphic processing  Units (GPU’s) | | . higher attention to privacy | .Contains noisy data |
| Author:  Faiza Masood  (2020) | | . Naïve bayes  . k-NN  . clustering  . decision ree algorithms  . random forest | . URL-based | | . efficient | . complicated and large dataset |
| Author:  G. Meghana  (2019) | | . Boosted linear model | . DDOS  . RFID attack  . spam city notes  . PCA | | . It detects spam parameters | . ambient features of iot devices |
| Author:  Guduru Jahnavi  (2020) | | . Bayesian Generalized Linear Model (BGLM) . boosted linear model | . Data mining  . cyber security | | . It is used to pre-process | . Acceptance of technologies is slow |
| Author:  Korivi Monishaa  (2019) | | . SVM  . K-NN  . RF  . naïve bayes  . ANN | . CSF  . PCA | | . allowed with a unconstrained outcome | . Trials are altered |
| Author:  Nebojsa Bacanin  (2020) | | . Logistic regression  . SGD | . XGBoost hyperparameters | | . improves the quality of randomness | . Should be tested on more real-world datasets |
| Author:  K V S Sai sharanya  (2019) | | . SVM  . naïve bayes  . K-NN  . ANN | . Functionality development  . stochastic filtering | | . easy retrieval | . Less performance issues |
| Author:  Avinash Ganne  (2020) | | . SVM  . KNN  . ANN  . NLP | . PSO method | | . uses cyber-attack detection . lead to more profits | . Risks are increased |
| Author:  Yeshi Paljor  (2018) | | . Naïve bayes  . KNN  . ANN  . RF | . Optical character recognition (OCR) | | . Highly effective | . less efficient |
| Author:  Samuel enseriban belanda  (2018) | | . SVM  . RF  . ANN  . DT | . Cognitive spammer  . voice over internet protocol(VOIP) | | . botnet detection frameworks | . risk of botnet attacks widely |
| Author:  Sonali kotni  (2018) | | . SVM  . RF  . ANN  . DT | . Bidirectional encoder representation from transformers (BERT)  . accuracy precision recall | | . data pre-processing techniques | . Transformers availability is the issue |
| Author:B.Thuraisingham(2020) | | . Deep learning  . artificial intelligence  . deep reinforcement learning | . Classification  . accuracy | | .introduces multisource information | . uncertainity |
| Author:  Kambham sravani  (2019) | | . Support vector machine(SVM)  . descion trees  . naïve bayes | . Radio frequency identification (RFID)  . Elliptic curve cryptography (ECC) | | . extra security | . Less payload |
| Author:  Praneeth netrapalli  (2019) | | . Guassian mixture models(GMMs) | . AUC Scores  . ROC  . CROC | | . provide a clearer idea | . insufficient to discard anomalies |
| Author:  Azmi jaafar  (2017) | | . Naïve bayes  . support vector machine(SVM)  . logitBoost | . Mapping assembly  . pre-filtering  . classification | | . Identify right performance | . inaccuracy in data |
| Author:  DR. Anoop kumar (2017) | | . Artificial neural networks (ANN)  . naïve bayes  . support vector machine(SVM) | . Simulation models | | . reduce process time and overhead | . efficiency |
| Author:  Yair Meidan  (2017) | | . Random forest(ensemble methods)  . support  vector machines(SVM) | . F1 score  . network interface cards (NICs) | | . Accuracy detection speed  . transportability | . Adversarial attacks |
| Author:  Poornima Mahadevappa (2019) | | . Logistic Regression (LR)  . Support  Vector Machine (SVM)  . nonlinear classifier  . Multi-Layer Perceptron (MLP) | . Linear Discriminant Analysis (LDA) | | . uses lightweight dimensionality technique | . Increases computational load to edge nodes |
| Author:  M.Arunkrishna (2019) | | . Artificial  Neural Networks  . Fuzzy Decision Tree | . Accuracy  . f-measure | | . highest accuracy | . Low performance |
| Author:  Chayan Halder  (2018) | | . Feed Forward Neural Network (FFNN)  . Multi Nominal Naive Bayes | . BERT  . LCS | | . texts are in the form of digital images | . not accurate |
| Author:  Noah apthrope  (2016) | | . k-nearest neighbours (KNN)  . random forest  . decision trees  . (SVM)  . neural networks | . Gini  impurity scores  . f-scores | | . high accuracy | . It uses limited feature set |
| Author:  Mr. A.Sanyasi Rao(2016) | | . Logistic regression K-. Nearest neighbours  . random forest  . naïve bayes | . Data preprocessing  . feature extraction | | . provides a universal feature set | . Not effectively identifying |

**3.3 Problem statement:**

The increase in IoT devices in various domains tends to increase spam attacks and lack of security.Detecting spam in real time further complicates the problem demanding for innovative approaches.

**4.RESEARCH OBJECTIVE:**

* In this review paper we aim to research different research papers and detects spam accuracy using different ML models.
* The paper aims to analyze and evaluate the existing research and methodologies to provide better understanding the current state of spam detection in IoT devices.

**4.1 GENERAL METHODOLOGY :**

Detects the accuracy, f-score, recall and support of different IoT devices using ML models. In the dataset we have 100000 rows and 32 features we have done feature Engineering on the data to generate accurate results. We are using five different ml algorithms such as support vector, randomforest, k-nearest neighbours and naïve bayes.

*DECISION TREE :*

Decision tree algorithms are a popular choice for classification and regression tasks in machine learning. They use a tree-like model to make decisions based on input features.

Training data n

Training data2

Training

Data1

Training

Set

Testing set

Decision tree n

Decision tree 2

Decision tree 1

Voting

prediction

Figure 1-Decision tree

RANDOM FOREST :

Random Forest has a classifier that have a number of different decision trees. The Dataset will be divided into different sub datasets and take average to improve the accuracy for the model.

dataset

prediction

prediction

prediction

Majority value taken

Majority value taken

Figure 2-Random forest

SUPPORT VECTOR MACHINE :

SVM is used for classification , regression .But mostly used in classification problems . The data is divided into categories and seperated by a boundary and creates classes the new data is compared and can be easily inserted into the correct category .This boundary is called as hyperplane .

KNN ALGORITHM:

K-Nearest Neighbour is a Supervised algorithms. When new data arrives the knn algorithms compares the new data with the previously ready to use data and divides new data points based on their nearest neighbours.

**5.EXPERIMENTAL WORK:**

5.1 EXPERIMENTAL SETUP:

*1.DATA COLLECTION:*We have collected the data from REFIT smart home dataset

Link: <https://www.kaggle.com/code/offmann/smart-home-dataset/notebook>

*2.DATA PREPROCESSING:*We have divided the dataset into testing and training datasets in the 80:20 ratio . 80% as train dataset and 20% as testing dataset . We have also divided the dataset into features and label . We have imported train\_test\_split function from sklearn .

**5.2 DATASET DESCRIPTION:**

This CSV file contains the data set contains of 32 columns & 10000 rows

The columns are as follows :

Barn, House overall, Furnace 1, gen, Furnace 2, Home office,

Kitchen 12, Fridge ,Wine cellar, Garage door , Kitchen[12],

Kitchen 14, Kitchen 38 [kW],Barn [kW],Well [kW]

Microwave, Living room, Solar, temperature, Dishwasher [kW], humidity

Icon, visibility, apparent Temperature, pressure, wind Speed, cloudCover,windBearing, door, precipIntensity, dewpoint, summary.

• House overall : House overall .

• Home office : The energy that is used by specific appliance energy.

• Fridge : The energy that is used by specific appliance .

• gen: The Energy that is developed by of solar or other power generation objects.

• Wine cellar : The energy that is used by particular devices.

• Garage : Energy used by specific appliance .

• Kitchen : The energy that is used in kitchen 1 .

• Furnace : Particular appliance energy.

• Barn : The energy that is used by specific appliance .

• Fridge : The energy that is used by fridge.

• Well : The energy that is used specific appliance .

• Living room: The energy that is used in living room.

• Solar : The power that is generated using solar panels.

• pressure: Air pressure is for bad weather and rising is for good climate.

• Temperature: It expresses the cold and hot .

• Humidity: It is the percentage of water vapour present in air.

• Visibility: It senses optical wide range .

• Apparent Temperature: It I used by humans, caused by air temperature, humidity.

• Fridge : The energy that is used by particular appliance .

• Wind Speed: Wind speed .

• Cloud Cover: Cloudiness or portion of sky covered by cloud.

• Wind Bearing: Direction from which wind is blowing .

. Class = Spam 1 or no spam 0.

**6.RESULTS:**

6.1 RESULTS TABLE:

|  |  |  |
| --- | --- | --- |
| **Machine learning technique** | **Accuracy** | **Confusion Matrix** |
| Support vector machine (SVM) | 0.989 | [[1978 0]  [ 22 0]] |
| Random forest | 1.0 | [[1978 0]  [ 0 22]] |
| KNN | 0.9965 | [[1975 3]  [ 4 18]] |
| Decision tree | 1.0 | [[1978 0]  [ 0 22]] |
| Naive bayes | 1.0 | [[1978 0]  [ 0 22]] |
| Gradient Boosting | 1.0 | [[1978 0]  [0 22]] |

Table 2- performance evaluation

6.2 RESULTS GRAPH:

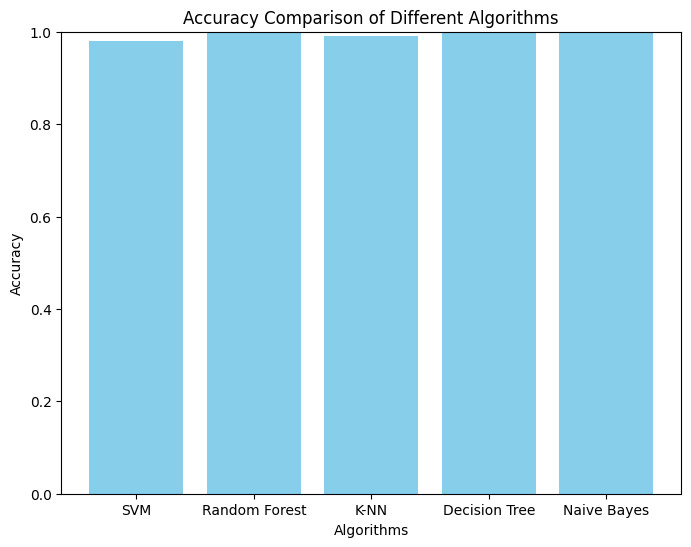
****

Figure 5- Result Graph

**6.3 DISCUSSION AND ANALYSIS:**

In this report we have used five different ml models for detecting spam in IOT devices like support vector (SVM), random forest, decision tree, KNN, naïve bayes. They all gave different accuracies and confusion matrices. Random forest, naïve bayes, and decision tree gave the highest accuracy as 1.0 whereas remaining, support vector machine and KNN gave 0.989 and 0.9965 % accuracies respectively.

**7.CONCLUSION AND FUTURE SCOPE:**

This detects the presence of spam in IoT devices using ML models. Here the system recognizes the spam limits of IOT contraptions utilizing ML models. This tells more about spam risks and secure device practices. The methods are used to protect user privacy while detecting the spam in IoT devices. After every model is used we predict the models accuracy, f1-score, recall and support. The model performance can be increased by using more data pre-processing techniques. They improves the IoT device performance and security. In future, this method is being improvised to attain best accuracy and to develop user friendly website to check spam on their own . Our goal is to make the weather and enveloping properties of IoT devices safer, secure, and more reliable in the future. This aims to create more privacy solutions for a secure IoT future. In future we intend to develop an application where users can directly check the presence of spam in their devices through online site and we intend to improve accuracies by applying advanced NLP and deep convolutional networks algorithm.

**8.REFERENCES:**

[1] Makkar, A., Garg, S., Kumar, N., Hossain, M. S., Ghoneim, A., & Alrashoud, M. (2020). An efficient spam detection technique for IoT devices using machine learning. *IEEE Transactions on Industrial Informatics*, *17*(2), 903-912.

[2] Sidharth, S., & Vasantha, S. AN EFFICIENT SPAM DETECTION TECHNIQUE FOR IOT DEVICES USING MACHINE LEARNING.

[3] Laique, H. M., & Morarjee, K. SPAM DETECTION FOR SMART HOME DEVICES USING VOTING CLASSIFIER AND ADABOOST.

[4] Rayan, A. (2022). Analysis of e-Mail Spam Detection Using a Novel Machine Learning-Based Hybrid Bagging Technique. *Computational Intelligence and Neuroscience*, *2022*.

[5 Rodrigues, A. P., Fernandes, R., Shetty, A., Lakshmanna, K., & Shafi, R. M. (2022). Real-time twitter spam detection and sentiment analysis using machine learning and deep learning techniques. *Computational Intelligence and Neuroscience*, *2022*.

[6] Reddy, M. D. M., Akshitha, M. P., Sowjanya, M. P., Kaveri, M. R., & Joshna, M. R. EFFICIENT ANOMALOUS DETECTION IN IOT SYSTEM USING MACHINE LEARNING.

[7] RANA, M. P., & PATIL, D. (2023). CYBER SECURITY THREATS DETECTION AND PROTECTION USING MACHINE LEARNING TECHNIQUES IN IOT. *Journal of Theoretical and Applied Information Technology*, *101*(7).

[8] Masood, F., Almogren, A., Abbas, A., Khattak, H. A., Din, I. U., Guizani, M., & Zuair, M. (2019). Spammer detection and fake user identification on social networks. *IEEE Access*, *7*, 68140-68152.

[9] Jayakumar, D., Srinivasan, S., Meghana, G., Harika, B. S., & Priya, K. Y. (2021). An eminent spam noticing methodology for IOT gadgets using ML techniques. *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS*, *11*(2), 2156-2166.

[10]Monishhaa, K., & Veeramallu, B. USING MACHINE LEARNING UNSOLICITED INFORMATION DETECTION TECHNIQUE FOR IOT DEVICES.

[11] Nookala Venu, D., Kumar, A., & Rao, M. A. S. (2022). Botnet Attacks Detection in Internet of Things Using Machine Learning. *NeuroQuantology*, *20*(4), 743-754.

[12] Doshi, R., Apthorpe, N., & Feamster, N. (2018, May). Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)* (pp. 29-35). IEEE.

[13] Tarafdar, A., Halder, C., & Dash, D. (2023). Spam Detection using Reference Text: A Preliminary Study for Spam Ground Truth Generation.

[14] Arunkrishna, M., & Mukunthan, B. (2020). A multiclassifier approach for twitter spam detection using innovative ann-fdt algorithm. *Indian Journal of Computer Science and Engineering*, *11*(5), 547-556.

[15] Mahadevappa, P., & Murugesan, R. K. (2021). A data quarantine model to secure data in edge computing. *arXiv preprint arXiv:2111.07672*.

[16] Meidan, Y., Bohadana, M., Shabtai, A., Ochoa, M., Tippenhauer, N. O., Guarnizo, J. D., & Elovici, Y. (2017). Detection of unauthorized IoT devices using machine learning techniques. *arXiv preprint arXiv:1709.04647*.

[17] Srivastava, A., & Kumar, A. (2022). Enhancement of Authentication in the IoT Network. *Journal of Algebraic Statistics*, *13*(3), 2328-2336.

[18] Sravani, K., & Swetha, A. Cryptography and Steganography Techniques for Securing Data in Internet of Things (IoT).

[19] Kotni, S., & Chandrasekhar Potala, D. L. S. SPAM DETECTION USING DEEP LEARNING MODELS.

[20] Nagaraju, B., & Saranya, K. S. Leveraging Machine Learning to recognize spamming in IoT systems.