**SPAM DETECTION IN IOT DEVICES:**

**1.ABSTRACT:**

Internet of the things is a group of millions of devices having sensors and actuators linked over wired or wireless channel for the data transfer in home. IOT enables the implementations between real-world objects irrespective of their locations geographically. IOT has been grown rapidly more than 25 billion devices. IOT devices produce large amount of data with different models having varying data quality. A lot of time and research has gone to effective ways to detect the forms of spams. Spam Identification in IoT utilizing ML Framework is suggested to accomplish this goal. With this increased usage and the demand, Smartphones play a key role in the user interface, providing access, control and backups A huge collection of input features sets is used to test five ML models. Machine learning algorithms ensure security and usability in IOT systems. Hackers use learning techniques to exploited weaknesses in intelligent IoT devices. To eliminate the generation of harmful input by IoT devices, a spam detection technique is proposed. the database is being split into multiple sets and provided as input to each method in the procedure. Here we used different machine learning techniques such as support vector machines (SVM), random forest, decision trees, naïve bayes, KNN performance of each classifier is analyzed. We use the spamcity score to detect the spam detection in Iot devices .Each model gives the spam accuracy .

**2.INTRODUCTION:**

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 applications need to protect data privacy to fix security issues such as intrusions, spoofing attacks, DoS attacks, DoS attacks, jamming, eavesdropping, spam, and malware.[1] This review paper aims to explore the topic of spam detection for IoT-based devices

One common approach is to use supervised learning algorithms[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 to train the data set and to predict 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 .each model computes a spam score .This score helps in letting us know the trustworthiness of each device under various parameters.The spam score is used to determine the reliability of each device in the smart home organization .This produces what conditions should be taken for efficient ,secure working of iot devices .Throughout the years the devices that are available on online are increasing and similarly the quantity of data produced by these devices will also increase.In this we use 5 machine learning models to evaluate spam score which determines the overall iot devices’s dependability .They have collected data from REFIT project .Here 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 in a smart home. They have used random forest and svm to evaluate the spam score for iot devices . To protect the IoT devices from producing the malicious information, the web spam detectionis targeted in this proposal. We have considered the machine learning algorithm for the detection of spam from the IoT devices.This proposals aims to reduce the spam occurence for these 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 .spam emails sent by different scammers pose potential concern for iot devices .y, bidirectional gated recurrent unit (BiGRU) and Convolution neural network (CNN) are combined with the Non-dominated Sorting Genetic Algorithm-II (NSGA II) multi-objective optimization method to effectively address imbalance problems.firsty they used CNN to extract features,used BiGRU to classify emails ,the data set was imbalanced to balance the data set the NSGA was imposed on data set.The accuracy of the model was increased .Different machine learning, data mining techniques are used in this project for cyber analytics for spam detection.They have used support vector machine algorithm extracted the features ,Cnn algorithm is used to extract color,shape,texture features,query image features a feature vector is generated which is further compared with all vector stored in database. There are drawbacks in the existing systems i.e; ot is less effective due to lack of spam detection in iot devices and it also has some merit/.advantages i.e, here the spam detection is validated from 5 different machine learning models. It computes spam score of each mode and then used for detection. The spamicity score used in this research is to determine the reliability of iot devices in smart home organisation. In future we can consider climatic and surrounding changes of iot devices to make more secure. Nowadays, emails are everywhere, they are used in every field, from business to education. Emails have 2 categories i.e; spam and ham. Here several machine learning techniques and deep learning techinques like naïve bayes, decision trees, etc. are used to spam filteration.

**3.2 Table:**

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

**RESEARCH OBJECTIVE :**

* The research objective of the review paper on spam detection in IoT devices using machine learning is to explore the effectiveness and limitations of various machine learning techniques in detecting spam attacks in IoT ecosystems
* The paper aims to analyze and evaluate the existing research and methodologies in order to provide insights into the current state of spam detection in IoT devices.

**4.GENERAL METHODOLOGY :**

Detects the spam parameters of IoT devices using machine learning models. The IoT dataset used for experiments, is pre-processed by using feature engineering procedure. By experimenting the framework with machine learning models , We are using Decision Tree ,Random Forest ,SVM ,kNN algorithms and predicts the spam in IOT devices .

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

Set

Testing set

Voting

(averaging)

prediction

RANDOM FOREST :

Random Forest is a classifier that contains a number of decision trees on various subsets of the given dataset and takes the average to improve the predictive accuracy of that dataset.

dataset

prediction

prediction

prediction

Majority value taken

Majority value taken

SUPPORT VECTOR MACHINE :

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. Mostly it is used for Classification problems in Machine Learning. The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.



KNN ALGORITHM:

K-Nearest Neighbour is one of the simplest Machine Learning algorithms based on Supervised Learning technique. K-NN algorithm assumes the similarity between the new data and available cases and put the new case into the category that is most similar to the available categories.



**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 split the dataset into training and testing datasets in the ratio of 80:20. 80% as train dataset and 20% as testing dataset . We have also divided the dataset into feature column and label column. We have imported train\_test\_split function from sklearn .

**5.2 DATASET DESCRIPTION:**

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

The columns are as follows :

[ 'gen [kW]', 'House overall [kW]', 'Dishwasher [kW]',

'Furnace 1 [kW]', 'Furnace 2 [kW]', 'Home office [kW]', 'Fridge [kW]',

'Wine cellar [kW]', 'Garage door [kW]', 'Kitchen 12 [kW]',

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

'Microwave [kW]', 'Living room [kW]', 'Solar [kW]', 'temperature',

'icon', 'humidity', 'visibility', 'summary', 'apparentTemperature',

'pressure', 'windSpeed', 'cloudCover', 'windBearing', 'precipIntensity',

'dewPoint', 'precipProbability']

• gen [kW]: Total energy generated by means of solar or other power generation resources

• House overall [kW]: overall house energy consumption

• Dishwasher [kW]: energy consumed by specific appliance

• Furnace 1 [kW]: energy consumed by specific appliance4

• Home office [kW]: energy consumed by specific appliance

• Fridge [kW]: energy consumed by specific appliance

• Wine cellar [kW]: energy consumed by specific appliance

• Garage door [kW]: energy consumed by specific appliance

• Kitchen 12 [kW]: energy consumption in kitchen 1

• Barn [kW]: energy consumed by specific appliance

• Well [kW]: energy consumed by specific appliance

• Microwave [kW]: energy consumed by specific appliance

• Living room [kW]: energy consumption in Living room

• Solar [kW]: Solar power generation

• temperature: Temperature is a physical quantity expressing hot and cold.

• humidity: Humidity is the concentration of water vapour present in air.

• visibility: Visibility sensors measure the meteorological optical range which is defined as the length of atmosphere over which a beam of light travels before its luminous flux is reduced to 5% of its original value.

• apparent Temperature: Apparent temperature is the temperature equivalent perceived by humans, caused by the combined effects of air temperature, relative humidity and wind speed. The measure is most commonly applied to the perceived outdoor temperature.

• pressure: Falling air pressure indicates that bad weather is coming, while rising air pressure indicates good weather

• wind Speed: Wind speed, or wind flow speed, is a fundamental atmospheric quantity caused by air moving from high to low pressure, usually due to changes in temperature.

• cloud Cover: Cloud cover (also known as cloudiness, cloudage, or cloud amount) refers to the fraction of the sky obscured by clouds when observed from a particular location. Okta is the usual unit of measurement of the cloud cover.

• wind Bearing: In meteorology, an azimuth of 000° is used only when no wind is blowing, while 360° means the wind is from the North. True Wind Direction True North is represented on a globe as the North Pole. All directions relative to True North may be called "true bearings.

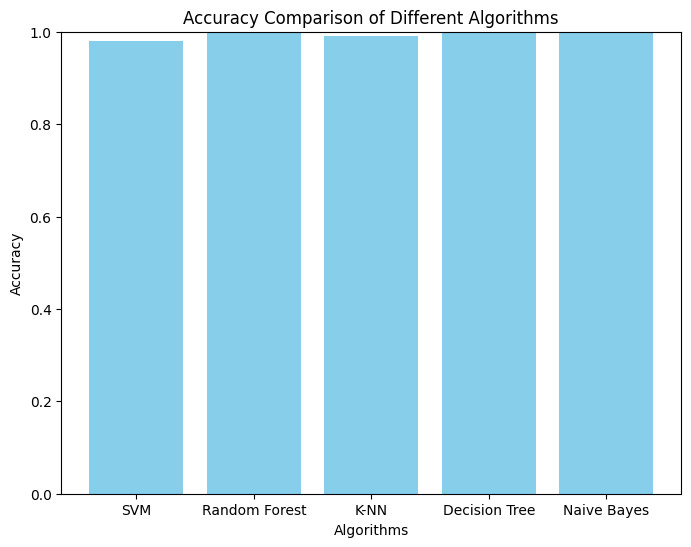
**.**Class= Spam 1 or no spam 0

**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]] |

6.2 RESULTS GRAPH:

****

6.3 DISCUSSION AND ANALYSIS:

In this report we have used five different machine learning techniques for detecting spam in IOT devices like support vector machine (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 percent accuracies respectively.

**7.CONCLUSION AND FUTURE SCOPE:**

The proposed framework detects the spam parameters of Iot devices using machine learning 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 experimenting on the five machine learning models every iot appliance is being awarded with spam score. The model performance can be increased by using more data pre-processing techniques. They improves the iot device performance and security. . In future work, this technique will be improved to achieve better accuracy. Our goal is to make the weather and enveloping properties of iot devices safer, secure, and more reliable in 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 website and we intend to improve accuracies by applying advanced NLP and deep convolutional networks algorithms .

**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.