Thesis: Title: Use of artificial intelligence and data analytics to compare the e-mail spam filtering (YAHOO, Gmail, Outlook) depending upon user experiences

Chapter # 2: Literature Review

Student Name: Shoaib

Contents

[Chapter # 2: Literature Review 3](#_Toc88225984)

[Introduction: 3](#_Toc88225985)

[Related Work 3](#_Toc88225986)

[Conclusion of Literature Review 14](#_Toc88225987)

[References 15](#_Toc88225988)

# Chapter # 2: Literature Review

## Introduction:

Literature review used to conduct the reviews of previous studies about the why, where and when it could be done, what are the major drawbacks in the previous studies and what are the advantages and disadvantages over the studies schemes. Literature review considering is part of secondary data collection method, it observer to highlight the research problem, research gaps, research area of interest to be happened on specific area and topics.

## Related Work

Email spam filtering method used to review the filtering method but due to lot of spams in the junk folder, so the Gmail considered is specialized spam detector that separate the spam mails in the junk mail folder, and it automatically deleted after some period of time. (Gbenga & StephenBassi, 2019, ) Machine learning for email spam filtering the method effectively works comparatively the email platforms, the issue is that the spam mails generates problem in the businesses and it difficult to tolerate in the daily usages of mails. The unwanted email considered as spam mails but it is very difficult to recognize that this mail is spam either or not in the junk of pool of mails, Microsoft outlook express mails does not handle spam filtering method due to poor framework of mails system. In recent years the development of machine learning method has been used to filter out the spam mails from the inbox as well as from the junk mail box. The application of machine learning method has been used by famous emails server such as Gmail, Yahoo, and outlook express, but the Gmail machine learning prediction method comparatively works well. The drawback of machine learning filtering exist in previous research but the replacement of deep learning model considered the best approach with the help of artificial neural networks layer. (Hanif Bhuiyan, 2018) Existing spam filtering method uses the machine learning method, email considering is most powerful and secure communication mechanism in the business dealing and serves the businesses over the world of commination. The increasing of data on daily basis detected through machine learning and automatically filter the unnecessary data from the emails server. various spam filtering method used in recent years to detect & filter the spam messages such as knowledge based method, clustering method, learning based method, and heuristic process. Machine learning method used such as Naïve bays, SVM, k-nearest neighbor, bays additive regression method, KNN tree method, python programming recognized one of popular framework to handle this problem.

(Jain & Bhargava, 2021) SPAM filtering using the artificial intelligence technique such as artificial neural network approach included with deep learning method approach considered is best approach, it works on millions of hidden layers to identify the exact layer which one is considered is required approach needed to extract the exact data that need to be filter out. The antispam filter method used by Gmail, Yahoo, Outlook service these mails severs uses the existing machine learning models to predict the spam mails, but the issues exist sometimes it’s not work efficiently, the arrival of hidden neural network layers change the strategies of machine learning prediction and its works efficiently comparatively to filter out the spams mails. Hidden neural networks layers approach works efficiently due to some hidden model building approach has been used. The algorithm detect, refine, separate and delete spams mails automatically after some period of time. (Dalkılıç & Sipahi, 2017) Spam filtering with sender authentication network, spam filtering method from the sender authentication that predict the senders in the mail list, it capture more spam mails, due to low resource difficult spam method has been implemented in recent years, spam mails is identify and filter in separate mail folder which effective way to identify them in separate folder. False positive and false negative method on the sender authentication list is help out to determine the spamming method. Sender policy framework protocol recognized well known origin method of spam filtering technique, due to sender authentication network developed to extend the spam filter recognize with sender IP address and network protocol , if the spam filtering method does not exist with comparison of false positive and false negative method, the way they are using to detect the spam on positive and negative layers mechanism of deep learning approach, result has been generated on false positive and false negative approach. (Aakash Atul Alurkar, 2019) Comparative analysis conducted to analyze the email spam classification technique using the machine learning approach. Gmail, Yahoo, Hotmail widely used by billions of people on daily, which connect all over the world people within a second. Machine learning approach has been widely used in all over the world, the detection of spam mails is detected on Google source platform in great efficiency the performance of mail sender and receiver has been recognized very well due to powerful mechanism of Google API with deep learning approach. Machine learning supervised learning and unsupervised learning method recognized on train and testing the models, the retrieving method approach through the API layers of machine learning models.

(Wang, 2012) The optimal design method based on hierarchal spam filtering method based on greylisting, the threats on emails is going beyond with normal email service than ever before. Present spamming method is used to block the spam mails but the deletion method does not exist in this year, the recognition of spam mails that recognize large number so spams mails. The overall hierarchical method used with greylisting approach which based on CBFG which uses three layers of filtering method. (Yang, et al., 2017 ) Describing and predicting enterprise email reply behavior based on small data sample collected from surveys, the automated mails generated by the consumer on enterprise level of application businesses, the commercial mails that used to predict with evidence on personal account mails activity in the organization. The evidence of predicating the emails automatically reply recognized on various factors due to various factors that generate reply to the customer on consumer behavior activities but the modelling of automatically replies mails works efficiently on various matter to generate various replies to the customer on dealing of business products and financial recovery. Developing model to predict the automatically sender replies and how it will take longs to take evaluation on it. The avocado emails collection describe the importance of automatically replies that based on thousands of avocado customer dealing on daily basis. (Hu, et al., 2021) The end to end encryption measurements on email spoofing attacks, phishing attack on emails recognized one of worst attack that hack email data due to sending spam mails and spam links which is dummy link that redirect on unknown website and steal the important user data. The cause of spam message attack on various organization enterprise email platform that does not contains particular security mechanism, email spoofing method uses to recognize the spam mails from the inbox. Studies show that the mails sender how is possible to scan the spoofing emails from the sender list. Penetrate mail box reach the defense on forged mails. 35 email providers tested the user reaction which was based on spoofing through the real world data on phishing email attack, email protocol uses to detect the spoofing such as Yahoo Mail, ICloud, Gmail uses the machine learning spoofing method to detect the unwanted mails from the inbox. Mostly the Gmail provides the end to end encryption that does not easily detect and hacked due to Google secure API layers comparatively Yahoo, Outlook does not provide the end to end encryption services.

(Bandaya & A.Mi, 2011) Analyzing the internet emails data through the method of email data spoofing, the spammers and phisher attacker readily availed to hack the enterprise emails data and get profit to send these data to other competitors. The above spam email to keep on top to generate the recipient mail box which aim to maximize the chance of action to detect & recognize the unwanted emails. The spoofing method can cause the confusion to recipient and it creates problematic situations over the client and customer to dealing with the kinds of data. (Sahni, 2021) Analysis of naïve bays algorithm uses in email spam filtering reviewing with the existing method approach that analyze the strength of machine learning prediction method as well as deep learning models prediction that ideally recognized as best method to detect and separate the spam messages and delete then particular time period. Author recommended that the approach of deep learning method is ideally works on predict the spam filtering method. The deep adversarial learning method effectively works on spam. (M., et al., 2016) email spam detection possible with using the best programming approach such as python machine learning models that predict and analyze the spam mails from the Gmail, Yahoo, Outlook express server. In these days all official correspondence possible through the emails service that communicating the official’s emails. The problem exists on internet due to spam email messages that used to waist the employee’s times due to unintentional detail and attraction of images and offers. Spam mails that uses unnecessary space of email server, and cause problem customer mails. The spam mails is mechanism of email phishing attack which used by the various industries to steal the important information of the organization and company asset details and other financial secret report. The machine learning approach with TFIDF algorithm term frequency inverse document approach implemented with support vector machine algorithm, result has been compared with confusion matrix of support vector algorithm with obtain the resultant accuracy of 99.9% of trained data and 98% testing data that obtain through the term frequency inverse document and support vector machine algorithm.

(CHARAN, 2021) Email classification using with machine learning prediction method ideally recognize the best approach due to increase number of unnecessary email on daily basis that increase the unwanted spams data on email servers and it uses to slow down the working of emails server. So there is need to creates an antispam filter that does not store any spam email in the inside the email inbox. In recent studies the development of machine learning spam filter widely used to detect and filter the spam emails. Machine learning based method effectively works to recognize the spam emails spam users it effectively works on Gmail, Yahoo, Outlook express to identify the any spam activities and spam email in these brands. The results shows that the existing machine learning method does not works effectively that requirement. So the achievement of deep learning method and deep adversarial learning method dealing with spam filter effectively. The future works required to works more efficiently to detect and delete automatically and does not stores inside the inbox and uses the email server memory. (Gangavarapu, et al., 2020) 99% accuracy of machine learning spam detection of unsolicited bulk mails, machine learning model has been extensively deploy by internet service providers and email service provider such as Yahoo, Gmail, Outlook uses machine learning python codes to detect and delete the spam messages in the email server. There are several phishing email attack occurred due to cyber security issues in the internet service providers domain. Email phishing attack uses to send spam email to users and it sends dummy link to redirect the user to another website which causes to steal the important information from the email. Email phishing attack identified with ethical hacking, spam emails not only wasting the user times it also consumes lot of internet bandwidth. Spam mail also contain some malware attack information which operate in windows operating system, various window operating system still not secure due to firewall breaches and built in antivirus was not providing the secure services to hide the windows data and files. The spam mail messages contain spam attachment which execute on window directory system 32 and slow down the working of operating system, so window technology still not well due to less security features in it. (Dada, 2018) Additionally the logistic model tree introduction machine learning method for email spam filtering, email spam uses to changes the behavior of employees email and steal the essential information which uses to beat the competitors. Machine learning approaches uses to solve the spam problem in most recognize internet service provider such as Yahoo, Google, Outlook server uses various machine learning and deep learning based technique to solves this issue in organize way. The conventional method of machine learning uses the black list strategies to block the spam ID over the internet services. IP addresses, domain services, was not able to identify the phishing threads so the programming interface uses the spam filtering and removing method to organize the enterprise application.

(Dada & Joseph, 2018) Random forest machine learning method for email spam filtering which is recognize best prediction method to spam emails. The traditional method widely uses in spam filtering such as black and white list uses the domain IP addresses which effectively works to detect the spam list and put it on black list. The high performance and reliable spam method which approach to successfully detect the email spam messages which detect the spam emails. The proposed random forest machine learning method which effectively works to detect and filter the spam message, objective was to detect the spam email from emails, the prediction accuracy with less number of features from the Enron public dataset contains 5180 emails on both ham, spam and normal emails. The set of prominent emails featured with extracted the apply the random forest algorithm method of machine learning with 99 % accuracy with false positive and false negative rate uses the weka data mining prediction software. (Shirani-Mehr & D. Delvia Arifin, 2016) Enhancing method to detect the spam email messages and mobile message the detection of mobile phone short messages service perform using FP-growth and Naïve bays classifier, the short messages services is still very popular due to communication medium sending services. SMS filtering performance by combining the two data mining task associated with classification and FP-growth. Utilizing the data mining approach in frequent patterns of SMS and naïve bays classifier algorithm is whether to identify the message is span or ham, using training and testing the sms dataset the naïve bays and FP growth produces the highest detect accuracy of 98.5% with improved precision score.

(Anon., , 2017, ) SMS spam detection using the H2o framework, various people receives spam messages over the mobile telephone which causes the problematic situations. SMS spam method already exist in previous research but the improved method requires to improve the performance of the detection method. Support vector machine and naïve bays algorithm and many other machine learning algorithm works to refine the working of email spam filtering which used to recognize the method of accurate F1 score and with highest rank of confusion matrix detection over the spam detection. The comparison between random forest and deep learning method uses to identify the various detection approach and accuracy of spam detection has been addressed in this studies. Result shows that the URL based text messages contain highest probability of detection due to internet API layers. The dataset uses from UCI machine learning repository, experiment results show the faster detection method spam detection, comparison of deep learning method contains highest scores random forest generate highest score with 50 trees and 20 depths including precision recall and F1-score 98% 96% 99% efficiency of detection. (NurAmir, et al., 2019, ) SMS spam messages detection using the term frequency inverse document and random forest tree algorithm deploy on sms spam messages data collection which is collected from machine learning UCI repository and kaggle platform. But the experiment results show that the detection of spam filtering accuracy is about to 97.50% accuracy of random forest tree algorithm.

(Sagar & Rutvij, 2020) In dealing with security and privacy concerns the machine learning uses the best prediction method to identify predict classify the security mechanism. Machine learning uses real time attack detection method with various API of python library packages to identify the real time problem and produces high quality accuracy. The real time decision making using the big data analytics approach is used to identify the approach of reduced cycle time of learning and cost efficiency including error free processing. (Onashoga, et al., 2015) An adaptive and collaborative server side sms spam filtering method with artificial immune system, existing system in 2015 does not able to stop the spam messages due to the problem exists on worldwide due to limited bag of training and validation method. Artificial immune system based on innate mechanism, user feedback and quarantine and tokenize the schemes of immune engine. Novel English corpus consisting of 5240 sms offering various studies including results show that the sms data with spam keywords. The 97% accuracy of artificial Bayesian with client side scripting to detect and spam sms and filter out in the mobile phone reserve user. (Islam & Ahmed, 2019) Social networking sites provides the Bangla text content through YouTube, the English text and Bangla text content combine schemes uses to spread the spam sms over the mobile phones users which is very difficult to identify them, the machine learning prediction model detect with 84% of accuracy including 70% F1 score and precision call.

(Maqsood, 2018) Microsoft .net library was used to detect the spam sms detection using the machine learning approach, the short sms on mobile phones users is also creating meta data that also engaged the user with annoying activity, the spam messages is widely consumes mobile users to engage mobile device and halt the operating system due to insufficiency memory of processing and rom. Random forest algorithm developed with C# programming it classify the dataset in terms of spam and ham. (Douzi, et al., 2020) Hybrid email spam detection model using the artificial intelligence neural network deep learning method to detect, separate and remove from the email. Its works very efficiently comparative other machine learning algorithm. The increasing volume of spam emails generated with essential of exact anti-spam filter detection method to detect unwelcome mails. The unwanted emails coming from other sources to beat the competitors and extract the secret data of the industries and also uses to steal the window operating system files and change with malware files. Author propose the hybrid model uses with artificial neural networks paragraph and vector distributed memory. The vector distributed model built the spam mails in background of resource to identify the spam sender. Conducted empirical research to identify the spam email problems including machine learning method.

(sewayaa, et al., 2021, ) the most accurate spam detection proceed with the machine leaning method which consider the accurate spam detection method, the algorithm of natural language processing which uses to analyze the email text and sender id that effective way to identify the spam text and spam sender. The machine learning natural language processing algorithm works on text mining to mine the text with lower case, upper case, special character including comma separated values. NLP algorithm able to identify the text within the spam and real messages. It also indicate the sender is fake or real. Author combines other method such as SVM, naïve bays, k-nearest neighbor, logistics regression, decision tree, random forest tree with accuracy result of 99% of spam mail detection (N. Kumar, 2020,) email spam basically in these days common problem for the every organization to meet this challenge various machine learning algorithm including deep learning logic to avoid spam mails. Email phishing attack sent via using the spam mails, the spam contains with dummy link and it redirect the user to another link and steal the information. For creating fake profiles, fake emails on social networking sites, it easily capture by the hackers and used for spam purposes. Phishing attack used in enterprise organization, spam user does not identify, mostly the spammers target the user which does not know the spam mails attack, the spammers objective is to commit fraud and steal essential information of the user, it might be used for human trafficking, so this thesis going to implement the spam email and spam user detector using the machine learning algorithm, so machine learning algorithm deploy in this work effectively to detect and filter the spam mail dataset with effective accuracy rate and precision call.

(Jun, et al., 2020) Spam detection approach used to detect the secure mobile message communication using the machine learning algorithms, mobile message communication is still insecure due to spam messages and spam calls. So the problem has been solved to deploy the machine learning spam detection method. Machine learning algorithm has been widely used by various researcher to meet spam messages, spam calls, spam email challenges. Machine learning classification algorithm implements to detect, clean and filter spam emails and spam messages such as K-Nearest neighbor, decision tree, logistic regression are used to classify the ham and spam messages in mobile device communication. The SMS spam message dataset is used for testing the method, further the dataset is divided into two parts such as training and testing purposes. The outcomes shows with absolute 99% accuracy for using KNN, DT, and LR. (Santoso, 2019) Additional the analysis part has been also tested with to verify the algorithm performance to detect and identify the machine learning email spam detection performance in the analysis phase accurately. Spam emails is very annoying email that take attention towards the other side and wasting the time of the person. Very few companies email accounts not the email server provides the feature of spam detection, email does not contain the facility to identify the spam id and spam messages. Network administrator separately added the module in the server to detect and filter the spam emails so the implementation workout to secure the user from the spam emails. Logistic regression, decision tree, random forest tree successfully deploy in separate module of the email server to detect the spammers and the efficiency requirement has been tested to deploy the machine learning algorithm in the email server. The training and testing part of spammers is also tested to deploy the machine learning method which proceed the highest detection accuracy score rate about 98%.

(Govil, et al., 2020) In today world, everything is considered as data and world of data science including artificial intelligence method. Rapid growing of data with rapid amount of email correspondence has been increased on daily basis. Widely used emails are commercial so these commercial emails might be able to spread email phishing attack with malware. So this time the malware execute in the system and slow down the memory and execute continual tasks and system does not respond towards the user requests. So this research show that the development of machine learning spam detection algorithm which used to separate the real emails and spam emails.

(Hirano & Kobayashi, 2019) Machine learning based ransomware detection using storage access patterns which is obtained from live-forensic hypervisor. The rapid increasing of internet of things devices including cloud service with cyber physical system, various cyber security attacks on enterprise and public sector, beside this ransomware attack damaged the UK National Health Service and various enterprises in the year 2017. Various researchers suggest solution to handle ransomware attack with prevention system. So to solve this ransomware attack problem the machine learning method has been used to avoid the ransomware attack problem. Ransomware attack samples data has been collected from forensic science center and it extensively used for testing purposes, the researcher first obtain the storage access patterns by using the samples of ransomware attack data hypervisor called waybackvisor. The suggested solution of ransomware attack to develop the machine learning algorithm such as K-Nearest, Support vector, random forest, decision tree with F-measure score about to 98% success rate. (Kumar, 2021 ) The novel machine learning method by using the emerging machine learning algorithm, machine learning is set of pattern that proceed to computer capable to learn without any programming effort. Machine learning support to validate the approach to support information. Machine learning algorithm works very fine to detect and clean the malware attack from the system. The functionality of machine learning method is used to detect the file either the malware is contain or not.

(Kumar, et al., 2018) Deep learning based image space detection various hackers and spammers employing to detect the obvious activity with spam image detection, spammers might be change the image and might be the original image fool the user, in this research the convolutional neural network method has been used to detect the spam image including the dataset of image 810 natural image and 928 spam image the classification accuracy achieved with about to 91.7%. (Akinyelu, 2021) Various advance method widely used to detect spam email messages and web spam detection, including social network spam various approaches has been widely used to inspired the working of email spam detection, mobile sms spam detection, web spam detection effectively detect filter out the spammers and hackers. (Singh, et al., 2021) The approach of email spam detection using the deep learning approach works efficiently by using the deep learning algorithm such as convolutional neural networks detect the image of spam messages by using the image dataset, beside this machine learning method used to detect and manage the spam email messages by using the Naïve bays, SVM, Decision tree, K-nearest neighbor algorithm and logistic regression method extensively used to detect the spam emails including the accuracy about 95% to 99% with successful F1 score and confusion matrix.

(Sharif, et al., 2020) Deep capture method used with deep learning method effectively to detect the spam email images and real images by using the image dataset. The dataset used from Kaggle repository and Github repository. Data augmentation possible to deploy the method of deep learning approach that effectively used to detect the real and fake emails. The convolutional neural network method used for detection of image data in the python library. The deep capture using the CNN algorithm which is part of deep learning algorithm that capture the image into billions of hidden layer with neural network. Neural network layer is construct with billions of hidden neural layer. Input layer, hidden layer, processing layer, output layer. These hidden layers match the pattern of image with evaluate to justify the exact pattern of image and get the exact result that required by the researcher. CNN network works on pattern of billions and millions of hidden neuron, the neural network architecture capture from the human brain like architecture that capture and make process the exact image by using the real world dataset and processed in more organize manner.

(Wu, et al., 2017) Twitter spam detection based on deep learning, proposed a machine learning based method to detect the spammers using the blacklisting method to detect the spamming activities on the twitter site. Recent method achieve 80% accuracy so the machine learning based method does not produce accurate result in 2017, so blacklisting method does not able to capture the spammers that required for accuracy. The novel method based on deep learning algorithm that the syntax of each tweet learned through wordvector training mode, then proceed to binary classifier which was based on presentation of dataset. The text based detection method detect the fake and spam tweets with activity of the twitter account, this method analyze the twitter data which based on text. (G. Chetty, 2019) Deep learning based spam detection system developed the model which is based on combination of the word embedding technique including neural network algorithm, the word embedding method allows that distribute the presentation of words. Deep learning method used to learn the feature of text within the document and present the embedding space and these method used to learn the text, the deep neural network analyze the text from the text document and separate the spam text in large corporate document at the enterprise level.

## Conclusion of Literature Review

In this studies the comprehensive literature has been used to analyze and predict the method of spam email messages detection including with spam email detection. Beside this spam mobile phone message data is also present in this studies, spam text document which is extensively used at corporate business level. Spam email that was issues of 2 Era, still the issue completely not resolved but the spammers and hackers are blacklisted in the email. The aim of this secondary data is used in this thesis and also used secondary data in this thesis to detect and filter the spam email using the python machine learning method. This thesis combines all of the machine learning method and present all of the spam email detection method in one research. Previously the works is not present accurately due to some incomplete library of data science and machine learning. This research method is going to detect and filter the spammer and spam emails in more effective way.

Method Used:

1. Machine learning method used to predict filter and remove spam email by using the spam email dataset.
2. Machine learning Algorithm such as Naïve Bays, Support Vector Machine, Logistics Regression, Random Forest Tree, Decision Tree ,K-Nearest Neighbor.
3. Deep learning method to detect spam images from image dataset Convolutional Neural Networks.
4. Running Python application that detect spam email and present the outcomes of real emails.

# References

Aakash Atul Alurkar, S. B. R., 2019. A Comparative Analysis and Discussion of Email Spam Classification Methods Using Machine Learning Techniques. *Applied Machine Learning for smart data analysis,* Volume 1, pp. 1-22.

Akinyelu, A. A., 2021. Advances in spam detection for email spam, web spam, social network spam, and review spam: ML-based and nature-inspired-based techniques. *Journal of Computer Security, ,* 29 (5), pp. 473-529, .

Anon., , 2017, . SMS Spam Detection using H2O Framework. *Procedia Computer Science,* Volume 113, pp. 154-161.

Bandaya, M. T. & A.Mi, F., 2011. Analyzing Internet e-mail date-spoofing. *Digital Investigation,* 7(3), pp. 145-153.

CHARAN, M. C. S., 2021. MAIL CLASSIFICATION USING MACHINE LEARNING. *Journal of Engineering Sciences,* 12(8), pp. 120-130.

Dada, E. G., 2018. Logistic Model Tree Induction Machine Learning Technique for Email Spam. *The Pacific Journal of Science and Technology ,* 19(2), pp. 96-100.

Dada, E. G. & Joseph, S. B., 2018. Random Forests Machine Learning Technique for Email Spam Filtering. *University of Maiduguri Faculty of Engineering Seminar Series,* 9(1), pp. 29-35.

Dalkılıç, G. & Sipahi, D., 2017. Spam filtering with sender authentication network. *Computer Communications,* Volume 98, pp. 72-79.

Douzi, S., AlShahwan, F. A. & Mouad., 2020. Hybrid Email Spam Detection Model Using Artificial Intelligence. *International Journal of Machine Learning and Computing,* 10(2), pp. 316-327.

G. Chetty, H. B. a. M. W., 2019. Deep Learning Based Spam Detection System," 2019. *International Conference on Machine Learning and Data Engineering (iCMLDE), 2019,,* pp. 91-96.

Gangavarapu, Tushaar & Jaidhar, 2020. Applicability of machine learning in spam and phishing email filtering: review and approaches. *Artificial Intelligence Review ,* 53(7), pp. 5019-5081.

Gbenga, E. & StephenBassi, D. J., 2019, . Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon Science Direct,* 5,(6), pp. 1-10.

Govil, N., Agarwal, K. & Varshney, A. B. a. A., 2020. A Machine Learning based Spam Detection Mechanism. *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), ,* pp. 954-957,.

Hanif Bhuiyan, A. A. T. I. J., 2018. A Survey of Existing E-mail Spam Filtering Methods Considering Machine Learning Techniques. *lobal Journal of Computer Science and Technology,,* p. 1.

Hirano, M. & Kobayashi, R., 2019. Machine Learning Based Ransomware Detection Using Storage Access Patterns Obtained From Live-forensic Hypervisor. *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS), ,* pp. 1-6.

Hu, H., Wang, G. & Tech, V., 2021. End-to-End Measurements of Email Spoofing Attacks. *27th Usenix Symposium,* 1(1), p. 1.

Islam, T. & Ahmed, S. L. a. N., 2019. Using Social Networks to Detect Malicious Bangla Text Content. *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), ,* pp. 1-4.

Jain, A. & Bhargava, N., 2021. SPAM Filtering Using Artificial Intelligence. *Wiley online library,* Volume 1, p. 1.

Jun, L. G., Nazir, S. & Khan, H. U., 2020. Spam Detection Approach for Secure Mobile Message Communication Using Machine Learning Algorithms. *Machine Learning and Applied Cryptography Security and communication networks,* Volume 1, p. 1.

Kumar, A. D. ；. K. A., 2021 . A New Malware Detection Model using Emerging Machine Learning Algorithms. *International Journal of Electronics and Information Engineering ,* 3(1), pp. 24 - 32 .

Kumar, A. D., R, V. & KP, S., 2018. DeepImageSpam: Deep Learning based Image Spam Detection. *Computer Vision and Pattern Recognition (cs.CV); Cryptography and Security (cs.CR),* p. 1.

M., R., Chowdary & Harith, N., 2016. EMAIL SPAM DETECTION USING PYTHON & MACHINE LEARNING. *Turkish Journal of Physiotherapy and Rehabilitation,* 3(1), pp. 1-4.

Maqsood, S. S. A. a. J., 2018. Net library for SMS spam detection using machine learning: A cross platform solution,. *2018 15th International Bhurban Conference on Applied Sciences and Technology (IBCAST),,* pp. 470-476.

N. Kumar, S. S. a. N., 2020,. Email Spam Detection Using Machine Learning Algorithms. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), ,* pp. 108-113.

NurAmir, N., SjarifNurulhuda & Azmi, F., 2019, . SMS Spam Message Detection using Term Frequency-Inverse Document Frequency and Random Forest Algorithm. *Procedia Computer Science,* Volume 161,, pp. 509-515.

Onashoga, A. S., O, O. & Adesina, 2015. An Adaptive and Collaborative Server-Side SMS Spam Filtering Scheme Using Artificial Immune System. *information security journals global perspective,* 24(6), pp. 1-24.

Sagar, R. & Rutvij, 2020. Applications in Security and Evasions in Machine Learning: A Survey. *Electronics Journal,* 9(1), pp. 1-97.

Sahni, R., 2021. Analysis of Naıve Bayes Algorithm for Email Spam Filtering. *IJMTST - International Journal for Modern Trends in Science and Technology (ISSN:2455-3778),* 7(1), pp. 5-9.

Santoso, B., 2019. An Analysis of Spam Email Detection Performance Assessment Using Machine Learning. *Jurnal Online Informatika ,* 4(1), p. 1.

sewayaa, Y. K., ovab, E. A. & monovb, A. A., 2021, . Evaluating the Effectiveness of Machine Learning Methods for Spam Detection. *Procedia Computer Science,* Volume 190, , pp. 479-486.

Sharif, B. K., bbaHyoung, A. & Kim, s., 2020. DeepCapture: Image Spam Detection Using Deep Learning and Data Augmentation. *Australasian Conference on Information Security and Privacy,* pp. 461-475.

Shirani-Mehr, H. & D. Delvia Arifin, S. a. M. A. B., 2016. Enhancing spam detection on mobile phone Short Message Service (SMS) performance using FP-growth and Naive Bayes Classifier,. *2016 IEEE Asia Pacific Conference on Wireless and Mobile (APWiMob), 2016,,* pp. 80-84.

Singh, A. P., Singh, A. & Chatterjee, K., 2021. A Comparative Approach for Email Spam Detection Using Deep Learning. *Intelligent Computing and Communication Systems ,* pp. 187-200.

Wang, Y., 2012. Optimal Design of Hierarchical Spam Filtering Method Based on Greylisting. *Applied Mechanics & Material,* Volume 1, p. 1.

Wu, T., Liu, S. & Zhang, J., 2017. Twitter spam detection based on deep learning. *ACSW '17: Proceedings of the Australasian Computer Science Week Multiconference January 2017 ,* Volume , pp. 1-3.

Yang, L., Dumais, S. T. & N, P., 2017 . Characterizing and Predicting Enterprise Email Reply Behavior. *SIGIR '17: Proceedings of the 40th International ACM SIGIR Conference on Research and Development in Information Retrieval ,* p. 235–244.