International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
Article Received: *25 December 2023* ***Revised:*** *12 January 2024* ***Accepted:*** *20 February 2024*

Identifying Online Spam Using Artificial Intelligence

Amit Goswami[1], Ripalkumar Patel[2], Chirag Mavani[3], Hirenkumar Kamleshbhai Mistry[4]
[1]Software developer, Source Infotech
[2]Software developer, Emonics
[3]Devops engineer, Dxc Technology
[4]Sr. System Administrator, Zenosys LLC
amitbspp123@gmail.com[1], Ripalpatel1451@gmail.com[2], chiragmavanii@gmail.com[3], hiren_mistry1978@yahoo.com[4]

Abstract: Preventing spam is becoming increasingly crucial as online commerce and communication grow quickly because it helps to keep people secure and websites reliable. Finding and lowering internet spam increasingly depends critically on artificial intelligence (AI). This paper describes how artificial intelligence detects spam now by use of methods like machine learning, language interpretation, and pattern recognition. AI can combine unsupervised approaches to identify odd behavior with supervised learning using labeled data. Among the difficulties include spotting fresh spam compositions and keeping precise real-time detection. By means of improved spam detection capability of artificial intelligence, researchers want to increase online platform security and thereby influence people's internet use.

Keywords: *Online Spam Detection; Artificial Intelligence, Machine Learning, Natural Language Processing, Anomaly Detection.*

1. INTRODUCTION

These days, our daily activities center on the Internet in some way. Mostly email, we use the Internet for many more reasons. As it makes online communication easier, email is utilized more and more. But when email usage increases as well, email spam increases. Spam is defined by massive amounts of unsolicited emails filling your inbox with advertisements and maybe harmful content.

Spam is annoying and sometimes dangerous, hence it is a problem. Often the result of marketing campaigns or scams aimed to deceive targets into revealing personal information is spam. Apart from being a nuisance, spam may undermine faith in online systems and facilitate cybercrimes such identity theft.

Spam is driven by the simplicity with which spammers might get email addresses from a variety of online sites. After gathered, these addresses are supplied in abundance and combined into large databases. Although spam might be bothersome, it is cheap and instantly attracts a lot of customers.

For consumers, spam is mostly frustrating. Spam clogs your email inbox and increases the difficulty of spotting real correspondence. Dealing with many unsolicited emails might not only waste time but also reduce production. Some types of spam, like links to fraudulent websites or downloads potentially compromising your computer, are also very dangerous.

Like the spread of spam, attempts against it have evolved. First, manually vetted and blacklisted known spammers But automatic replies were crucial as spammers developed more sophisticated techniques like social engineering and obfuscation. Here machine learning (ML) and artificial intelligence (AI) take front stage. These technologies search enormous amounts of email data looking for spam from actual correspondence. Look for patterns in your email content that indicate suspicious links or spam-like words.

Spam filters powered by AI use many methods to determine whether we have spam or genuine mail. Guide your choices with data models, including examples of spam and legitimate email. Natural language processing (NLP) systems also improve their effectiveness by identifying unusual phrases and links that indicate hostile intent. These filters also check for abnormal real-time activity that may indicate a possible spam attack.

Good spam management is still a challenge even with the advancement of technology. The continuous method varies from spammer to spammer to avoid continuous improvement of spam filter detection calls. Finding the perfect balance between accurately detecting spam and minimizing false positives, ie. emails incorrectly classified as spam, helps ensure that customers receive the relevant information without interruption. to make sure it's not too serious.

In expansion to being hurtful, spam may be a danger to web foundation and cyber security. Large-scale spam campaigns can overpower e-mail foundation and devour transmission capacity and capacity required by genuine applications that bolster authentic movement. This burden influences not as it

were service providers, but too working costs and, within the most severe cases, user inconvenience.

Spam is more than fair a disturbance. Spam may be a vector that leads to information breaches and cyber assaults. For illustration, phishing messages are sent to trustworthy companies in an endeavor to trap shoppers into uncovering delicate data such as passwords or bank subtle elements. Spam can too contain joins to pernicious websites outlined to misuse shopper computer bugs, encouraging the spread of malware and ransomware. Organizations and people utilize diverse procedures to diminish the dangers related with spam.

In addition to AI-powered filters that act as the first line of defense against spam, it's important to educate users to recognize phishing attacks and follow safe email practices. Regularly updating your security software and complying with legal measures such as the CAN-SPAM Act and GDPR can help you regulate your email practices and protect the privacy of your users.

The future of anti-spam will evolve as technology and cybersecurity practices evolve. AI and ML are expected to play a key role in improving spam detection by using big data analytics and predictive modeling to effectively predict and combat new spam tactics. In addition, the industry must develop comprehensive strategies to respond to the multifaceted challenges posed by spam..

2. REVIEW OF WORKS

Almeida, Gomez, and Yamakami's 2010 work focuses on SMS spam filtering but offers basic techniques that may also be used to identify email spam. They spoke about methods for feature selection and classification, which provide the groundwork for understanding more general applications in spam detection.

An method to email spam filtering based on constructive improvement was proposed by Carreras and Marquez (2001). Their efforts to improve weights centered on misclassified instances have been emphasized in the organizing of the 'Conference Meeting on Recent Advances in Natural Language Processing', and show how effective this method is in increasing classification accuracy.

In a paper published in Applied Intelligence, Kotsiantis, Tzelepis, and Pintelas (2007) investigated association rule-based filtering strategies for email categorization. In arrange to successfully distinguish spam, they highlighted the esteem of distinguishing shared designs and connections in mail content and metadata as an elective to routine machine learning methods.

In their 1998 article, Sahami et al. displayed a credulous Bayesian calculation for e-mail spam sifting, expanding its effortlessness based on relative probability and inferential probability to portray states fundamental quality representations. Their groundbreaking investigate appears that Gullible Bayes could be a dependable and versatile strategy for spam discovery.

Androutsopoulos et al. (2000) compared several attribute representations to make strides classification precision to assess the viability of Gullible Bayes in mail spam sifting. The consider highlights the algorithm's quality in overseeing enormous information sets and adjusting to changing spam strategies.

Proceeding their prior work, Androutsopoulos, Paliouras, and Vrachnos (2006) compared memory-based learning calculations with Naive Bayes for spam sifting. They concluded that Credulous Bayes could be a less difficult approach, in spite of the fact that memory-based strategies can give superior comes about and adjust preparing effectiveness and classification exactness. Their investigate appears that these two strategies can make strides specialized execution when they work together.

The versatile dispersed framework "Experience" was made by Dalvi et al. (2004) with mail spam sifting applications. Their work addresses the challenges of viably overseeing expansive volumes of mail and gives versatile arrangements to make strides spam discovery frameworks.

For e-mail sifting, Platt (1999) explored bolster vector machines (SVM), centering on procedures that progress demonstrate execution and speed up preparing. Much appreciated to his work, SVMs perform reliably in high-dimensional highlight spaces, making them reasonable for both genuine separation and spam.

In 2019, Li, He, Guo, Liu and Zhao explored how well repetitive neural systems (RNN) and convolutional neural systems (CNN) perform as profound learning structures for mail spam detection. They highlighted how profound learning can reveal complex designs in e-mail metadata and substance that can make strides the precision of spam location.

Bharti, Singh and Malhotra (2019) proposed a machine learning strategy for spam discovery utilizing ideal qualities. A survey of numerous classifiers and highlight determination strategies highlights the importance of feature plan in making strides spam location.

Kaur and Kaur (2020) displayed a comprehensive study of machine learning-based e-mail discovery frameworks, covering different calculations and determination strategies.

Their upgrade clarifies the improvement and current state of spam location innovation and includes to past investigate.

Prasad and Pal (2010) proposed a multi-algorithm machine learning approach for email spam detection. Their goal is to combine many classifiers to improve the overall classification accuracy and empathy of different spamming techniques.

Mishra, Joshi, and Gaur (2020) provide an in-depth study of machine learning for email spam detection. They looked at a lot of previous research to explain how spam detection works. They discussed several algorithms and methods to identify important aspects.

In order to identify spam emails, Saini and Kumar (2020) contrasted Random Forest, SVM, and Naive Bayes. To examine how these techniques choose the best characteristics and function, they were tested on many sets of data. They also offered suggestions for improving spam email detection.

In 2021, Ahirwal and Kaushik examined in great detail how machine learning may identify spam emails. They covered many applications of these systems, what traits to look for, and how to gauge their effectiveness. They discussed what has changed, what remains challenging, and what this field of study can do next.
To determine which algorithms to utilize for identifying spam emails, Rani and Nasa (2021) experimented with many approaches. Finding the best ones for this task, they examined K-nearest neighbors, decision trees, and Naïve Bayes. Ayyalasomayajula et al., in their research work published in 2019, provided key insights into the cost-effectiveness of deploying machine learning workloads in public clouds and the value of using AutoML technologies. Ayyalasomayajula et al., 2021, provided an in-depth review of proactive scaling strategies to optimize costs in cloud-based hyperparameter optimization for machine learning models. Authors Boozary, Payam et. al. discussed the impact of marketing automation on consumer buying behavior in the digital space via artificial intelligence. Every one of these research advances our knowledge on how to identify spam in emails. They demonstrate for us what is effective and what needs improvement. Their primary objectives are to protect emails from spam and to advance the state of spam prevention research.

3. PROPOSED METHODOLOGY FOR IDENTIFYING SPAM

The growing volume of unsolicited spam emails that clog our inboxes is the issue at hand. Businesses suffer monetarily as well as having to use up priceless internet resources. Spam is lucrative for those who send it even in spite of attempts to stop it. Strict channels some of the time misclassify genuine emails as spam, lost critical messages or conceivably commercial emails.

Current rule-based spam channels as a rule incorporate records of known spam addresses or the choice to as it were acknowledge mail from trusted sources. Be that as it may, these are barely secure procedures. Spammers can effectively alter mail addresses that will moreover show up to be genuine utilizing phishing procedures. Keeping these directions up to date requires a part of work and cash.

Normal dialect handling (NLP) and machine learning offer reasonable answers to these issues. These frameworks may utilize designs and characteristics of e-mail substance to decide whether or not we have spam. Since it can learn and adjust to modern sorts of spam, this strategy is more adaptable than settled criteria and decreases the chance of genuine emails being erroneously stamped as spam.

In our unused framework, we utilize K-Nearest Neighbors (KNN), Back Vector Machines (SVM) and Credulous Bayes. These programs ought to work way better than what we as of now have. We need to speed up and rearrange mail sifting with these modern innovations. In this way, unwanted emails are ensured and the proper ones reach the aiming beneficiaries.

Characteristic Dialect Handling (NLP) is another apparatus our framework employments to ponder and get it mail trades.. Its method of identifying spam from non-spam emails is word analysis. This helps us distinguish between legitimate and potentially spam communications more effectively. That makes it less prone to error.

Our goal is to use machine learning and natural language processing to create a system smart enough to block spam so that everyone can use email safely..

4. RESULTS

•To launch the project file, open the Jupyter Notebook prompt and go to the folder containing the project files, as seen in the Figure 1 below:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
Article Received: *25 December 2023* ***Revised:*** *12 January 2024* ***Accepted:*** *20 February 2024*

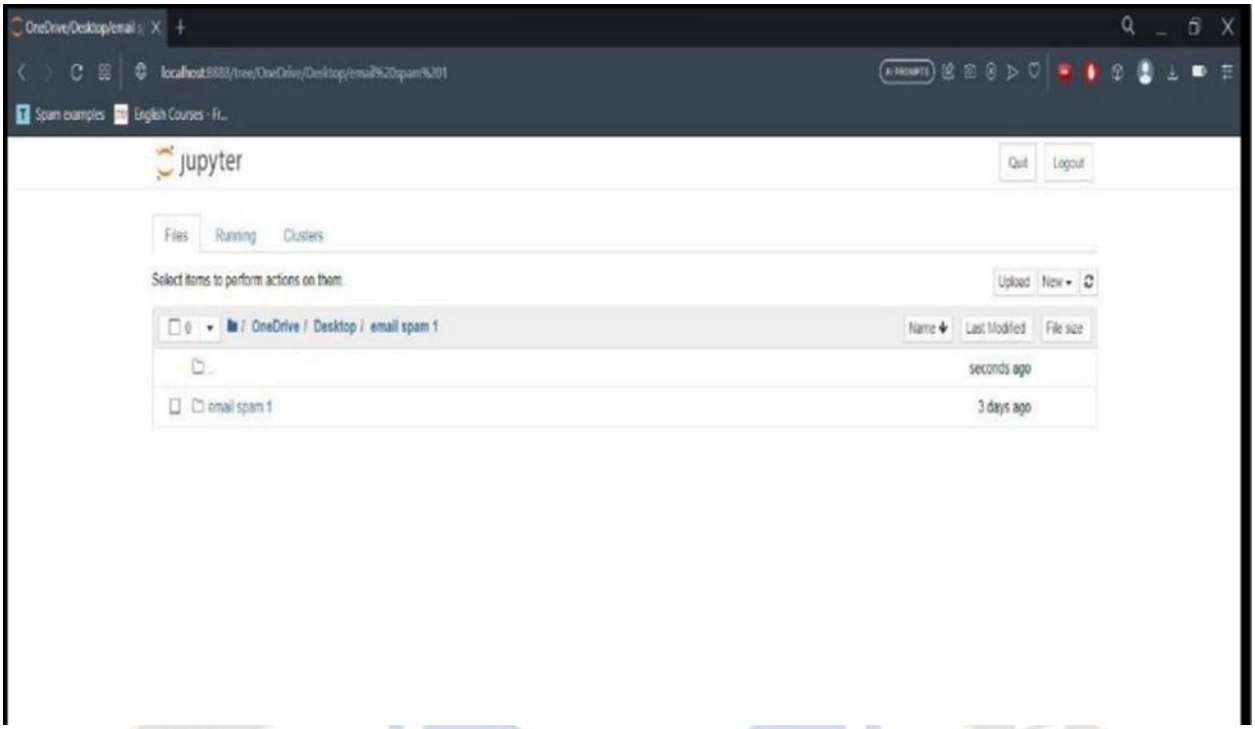

Fig.1: Opening Project File

• You must open the file in the following figure after modifying the directory as shown in the Figure 2:

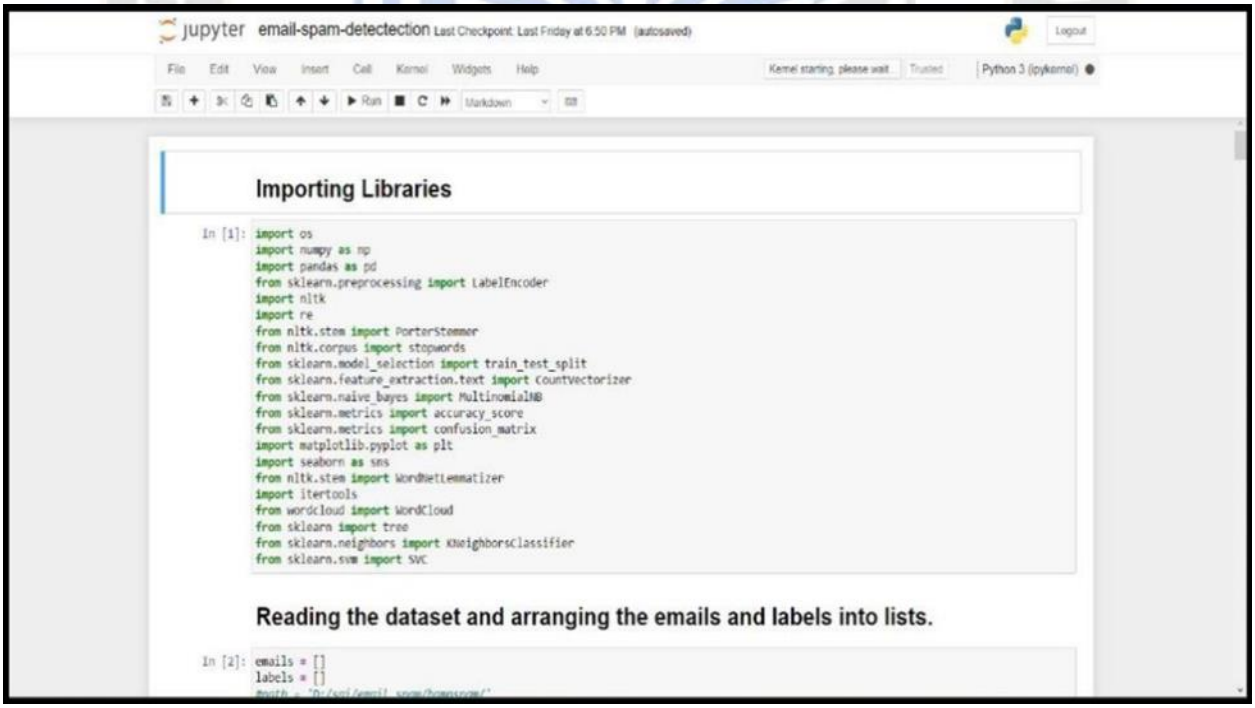

Fig.2:Changing The Directory

• Select "restart and run all" after clicking on the kernel as depicted in the Figure 3:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
Article Received: *25 December 2023* ***Revised:*** *12 January 2024* ***Accepted:*** *20 February 2024*

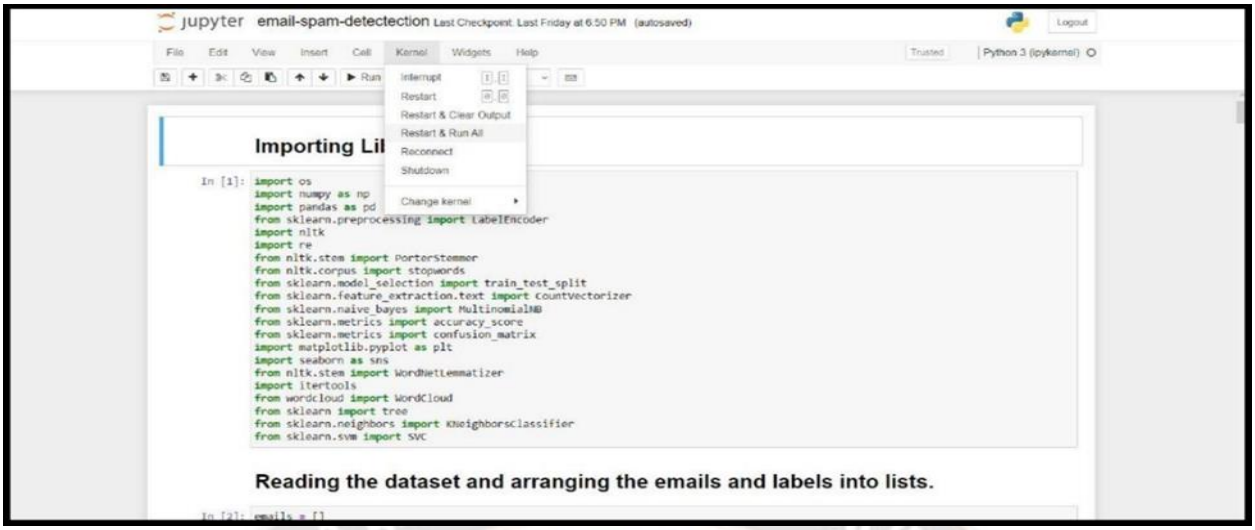

Fig.3: Execution Of The Project

• After waiting for a while for the code to run, input the text you want to determine is spam or ham in the prediction template and click run, as shown below in Figure 4:

Fig.4:EnterTheStiring

• Ham will appear as shown below if the message is about ham, illustrated in Figure 5:

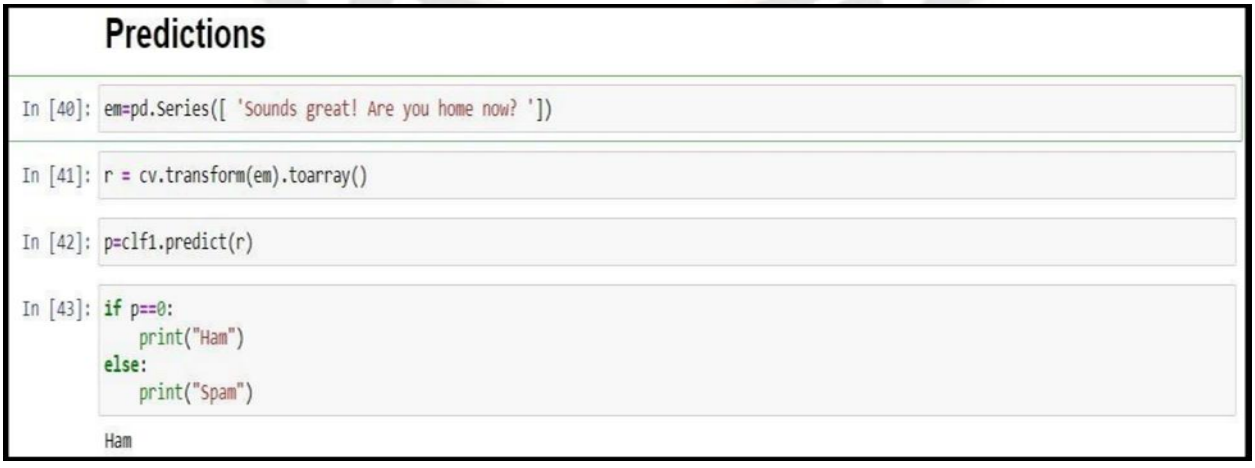

Fig.5: Prediction Of Ham

• Spam will appear in the message as shown below if it is spam shown in Figure 6:

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 12 Issue: 2
Article Received: *25 December 2023* ***Revised:*** *12 January 2024* ***Accepted:*** *20 February 2024*

Fig.6: PredictionOfSpam

6. CONCLUSION

In conclusion, machine learning (ML) and natural language processing (NLP) techniques are strong tools for sorting out spam emails. Using supervised learning algorithms such as Naive Bayes, Support Vector Machines (SVM) and K-Nearest Neighbors (KNN) and steps such as tokenization, common word removal and word reduction to their basic form, we can create highly accurate spam filters.

These channels can naturally discover and erase undesirable emails based on these messages. In our arrange, the precision of Gullible Bayes is 99%, SVM is 98%, and KNN is 97%. Gullible Bayes is the foremost precise of these, making it our best choice for spam discovery.

ML and NLP strategies are not as it were able of finding common spam designs; they can moreover bargain with more progressed spam such as phishing and phishing. By carefully analyzing the substance of an e-mail, these advances can identify little points of interest that show whether we have spam or veritable e-mail. This makes a difference guarantee that important messages reach the proper individuals without inadvertently being checked as spam.

Spam channels that utilize machine learning (ML) and characteristic dialect preparing (NLP) would be exceptionally valuable. Naturally categorizing emails not as it were spares you time, but moreover progresses the productivity of your inbox. In expansion, it keeps your emails secure by blocking pernicious substance and guaranteeing the unwavering quality of your communications. All in all, utilizing machine learning and normal dialect preparing to oversee mail spam is an imperative step in making the web more secure. In today's computerized world, it makes a difference people and businesses to move forward the security of their emails, rearrange communication and make strides the utilize of assets...

REFERENCES

[1]. Shukor Bin Abd Razak, Ahmad Fahrulrazie Bin Mohamad “Identification of Spam Email Based on Information from Email Header” 13th International Conference on Intelligent Systems Design and Applications (ISDA), 2013.

[2]. Mohammed Reza Parsei, Mohammed Salehi “E-Mail Spam Detection Based on Part of Speech Tagging” 2 nd International Conference on Knowledge Based Engineering and Innovation (KBEI), 2015.

[3]. Sunil B. Rathod, Tareek M. Pattewar “Content Based Spam Detection in Email using Bayesian Classifier”, IEEE ICCSP 2015 conference.

[4]. Aakash Atul Alurkar, Sourabh Bharat Ranade, Shreeya Vijay Joshi, Siddhesh Sanjay Ranade, Piyush A. Sonewa, Parikshit N. Mahalle, Arvind V. Deshpande “A Proposed Data Science Approach for Email Spam Classification using Machine Learning Techniques”, 2017.

[5]. Kriti Agarwal, Tarun Kumar “Email Spam Detection using integrated approach of Naïve Bayes and Particle Swarm Optimization”, Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS), 2018.

[6]. Cihan Varol, Hezha M. Tareq Abdulhadi, “Comparison of StringMatching Algorithms on Spam Email Detection”, International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism, Dec. 2018.

[7]. Duan, Lixin, Dong Xu, and Ivor Wai-Hung Tsang. "Domain adaptation from multiple sources: A domain dependent regularization approach." IEEE

Transactions on Neural Networks and Learning Systems 23.3, 2012.

[8]. K. S. Adewole, N. B. Anuar, A. Kamsin, K. D. Varathan, and S. A. Razak, "Malicious accounts: dark of the social networks," Journal of Network and Computer Applications, vol. 79, pp. 41–67, 2017.

[9]. A. Barushka and P. Hájek, "Spam filtering using regularized neural networks with rectified linear units," in Proceedings of the Conference of the Italian Association for Artificial Intelligence, Springer, Berlin, Germany, November 2016.

[10]. F. Jamil, H. K. Kahng, S. Kim, and D. H. Kim, "Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms," Sensors, vol. 21, no. 5, p. 1640, 2021.

[11]. M. H. Arif, J. Li, M. Iqbal, and K. Liu, "Sentiment analysis and spam detection in short informal text using learning classifier systems," Soft Computing, vol. 22, no. 21, pp. 7281–7291, 2018. [12] I. Rish, "An empirical study of the naive Bayes classifier," in IJCAI 2001 Workshop on Empirical Methods in Artificial Intelligence, University of British Columbia, Computer Science Department, Vancouver, Canada, 2001.

[12]. N. F. Rusland, N. Wahid, S. Kasim, and H. Hafit, "Analysis of Naïve Bayes algorithm for email spam filtering across multiple datasets," in Proceedings of the IOP Conference Series: Materials Science and Engineering, IOP Publishing, Busan, Republic of Korea, 2017. [14] A. K. Sharma and S. Sahni, "A comparative study of classification algorithms for spam email data analysis," International Journal on Computer Science and Engineering, vol. 3, no. 5, pp. 1890–1895, 2011.

[13]. Androutsopoulos, I., Koutsias, J., Chandrinos, K. V., Paliouras, G., & Spyropoulos, C. D. (2000). An evaluation of naive Bayesian anti-spam filtering. Proceedings of the Workshopon Machine Learning in the New Information Age, 1(1-3), 9-17.

[14]. Drucker, H., Wu, D., & Vapnik, V. N. (1999). Support vector machines for spam categorization. IEEE Transactions on Neural Networks, 10(5), 1048-1054.

[15]. Bao, X., Zhang, Y., Li, Q., Yang, Z., & Zhang, W. (2014). A hybrid approach to spam email detection using improved ant colony optimization and support vector machine. Information Sciences, 277, 495-511.

[16]. Su, C. M., Li, W. J., & Lee, C. C. (2015). An ensemble-based classifier for email spam detection using weighted majority voting. Knowledge-Based Systems, 80, 136-145.

[17]. Selvi, S. T., & Radhika, R. (2017). Ensemble classifier with modified random forest for spam email detection. Journal of Computational Science, 21, 108-116.

[18]. Sun, J., Ma, J., Zeng, D., & Li, H. (2017). Email spam detection using a hybrid machine learning method. Information Processing & Management, 53(2), 427-437.

[19]. Le, H. V., Nguyen, M. T., & Nguyen, T. T. (2018). Email spam detection based on ensemble learning of extreme learning machine. International Journal of Machine Learningand Cybernetics, 9(4), 591-602.

[20]. Poon, C. K., & Domingos, P. (2009). Unsupervised spam detection using coherence propagation. Proceedings of the 12th International Conference on Artificial Intelligence and Statistics (AISTATS), 18, 465-472.

[21]. Perez-Macias, J. M., Araujo, L., & Travieso-Gonzalez, C. M. (2012). On the use of machine learning techniques for email spam filtering. Expert Systems with Applications, 39(10), 9570-9576.

[22]. Yang, L., & Zhang, L. (2012). A linear programming approach for email spam detection. Knowledge-Based Systems, 26, 151-159.

[23]. Almeida, T. A., Gómez, H. F., & Yamakami, A. (2010). Contributions to the study of SMS spam filtering: New collection and results. Journal of Machine Learning Research, 11, 3611-3628.

[24]. Carreras, X., & Marquez, L. (2001). Boosting trees for anti-spam email filtering. Proceedings of the Conference on Recent Advances in Natural Language Processing, 9-15.

[25]. Premkumar Reddy, Yemi Adetuwo and Anil Kumar Jakkani, Implementation of Machine Learning Techniques for Cloud Security in Detection of DDOS Attacks, International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp.25-34. doi: https://doi.org/10.17605/OSF.IO/52RHK

[26]. Adeola Agbonyin, Premkumar Reddy, Anil Kumar Jakkani, Utilizing Internet of Things (IOT), Artificial Intelligence, and Vehicle Telematics for Sustainable Growth in Small, and Medium Firms (SMES), International Journal of Computer Engineering and Technology (IJCET), 15(2), 2024, pp. 182-191. doi: https://doi.org/10.17605/OSF.IO/QX3DP

[27]. Srivastava, Pankaj Kumar, and Anil Kumar Jakkani. "FPGA Implementation of Pipelined 8× 8 2-D DCT and IDCT Structure for H. 264 Protocol." 2018 3rd International Conference for Convergence in Technology (I2CT). IEEE, 2018.

[28]. Srivastava, P. Kumar, and A. Kumar Jakkani. "Android Controlled Smart Notice Board using IoT." International Journal of Pure and Applied Mathematics 120.6 (2018): 7049-7059.

[29]. Boozary, Payam. "The Impact of Marketing Automation on Consumer Buying Behavior in the Digital Space Via Artificial Intelligence." Power System Technology 48.1 (2024): 1008-1021.

[30]. Ayyalasomayajula et al., Madan Mohan Tito "Proactive Scaling Strategies for Cost-Efficient Hyperparameter Optimization in Cloud-Based Machine Learning Models: A Comprehensive Review." ESP Journal of Engineering & Technology Advancements, vol. 1, no. 2, 6 Dec. 2021, pp. 43-56.

[31]. Ayyalasomayajula et. al., Madan Mohan Tito. "A Cost-Effective Analysis of Machine Learning Workloads in Public Clouds: Is AutoML Always Worth Using?" International Journal of Computer Science Trends and Technology (IJCST), Oct. 2019.