IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

# Email Spam Detection using Machine Learning

**Prof. Pranita Mokal, Onkar Ghate, Abhishek Gadhave, Pooja Bairagi, Sakshi Jadhav**
Department of Information Technology
G H Raisoni institute of Engineering & Technology, Pune

**Abstract:** Today, email and message spam remains a significant issue, and it can cause various problems such as clogging up inboxes, reducing internet speed, and potentially compromising personal information. Researchers and organizations continuously work on developing techniques to identify spammers and spammy content to mitigate these issues. One approach commonly used for spam detection is applying machine learning algorithms, such as SVM Algorithm, to classify messages as either spam or non- spam (ham). These Algorithm calculate the probability of a message being spam or ham based on the presence of certain features or keywords. By training the classifier on a labelled dataset of known spam and ham messages, it can learn to make predictions on new, unseen messages. In addition to content analysis, other techniques may also be employed to identify spam, including analysing the Sender's IP address, checking for patterns of mass distribution, examining the email header information, and utilizing reputation-based systems that track the behaviour of known spammers. However, it's important to note that spammers continually evolve their tactics to bypass spam filters and detection systems. As a result, spam filters need to be regularly updated and improved to stay effective. Additionally, legitimate emails can sometimes be mistakenly flagged as spam, so there is a trade-off between accurately identifying spam and avoiding false positives. Overall, spam detection and combating spam remain active areas of research and development in the field of cyber security. The aim is to refine techniques and employ advanced technologies to minimize the impact of spam and protect users from its negative consequences.

**Keywords:** message spam

## REFERENCES

**[1].** H. Faris, A. M. Al-Zoubi, A. A. Heidari et al., "An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks," Information Fusion, vol. 48, pp. 67–83, 2019.

**[2].** E. Blanzieri and A. Bryl, "A survey of learning-based techniques of email spam filtering," Artificial Intelligence Review, vol. 29, no. 1, pp. 63–92, 2008.

**[3].** Alghoul, S. Al Ajrami, G. Al Jarousha, G. Harb, and S. S. Abu- Naser, "Email classification using artificial neural network," International Journal for Academic Development, vol. 2, 2018.

**[4].** N. Udayakumar, S. Anandaselvi, and T. Subbulakshmi, "Dynamic malware analysis using machine learning algorithm," in Proceedings of the 2017 International Conference on Intelligent Sustainable Systems (ICISS), IEEE, Palladam, India, December 2017.

**[5].** S. O. Olatunji, "Extreme Learning machines and Support Vector Machines models for email spam detection," in Proceedings of the 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), IEEE, Windsor, Canada, April 2017.

**[6].** J. Dean, "Large scale deep learning," in Proceedings of the Keynote GPU Technical Conference, San Jose, CA, USA, 2015.

**[7].** J. K. Kruschke and T. M. Liddell, "Bayesian data analysis for newcomers," Psychonomic Bulletin & Review, vol. 25, no. 1, pp. 155–177, 2018.

**[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.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

**[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