International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 12, Issue 01, January 2023)

A Survey on Spam Identification Mechanism in Iot Network using AI Techniques

Vishnu Kumar Tiwari[1], Ram Gopal Yadav[2]
[1,2]*Assistant Professor, Compucom Institute of Information Technology and Management, Jaipur, India*

***Abstract*— A side effect of the growth of the artificial intelligence sector has been security concerns. Since machine learning has the potential to mine the value of big data, it has been widely employed for fraud detection, spam detection, and harmful file identification. However, there is a tremendous incentive for hostile attackers to circumvent such methods. Attackers can only use a black box attack because they are unaware of the precise specifications of the machine model. In this study, machine learning-based spam detection methods for Internet of Things devices are reviewed.**

***Keywords*—Spam, Machine, IOT, Detection, Security, AI.**

I. INTRODUCTION

The Internet of Things (IoT) is a collection of millions of gadgets with sensors and actuators connected via wired or wireless channels for data transmission. Over 25 billion linked devices are anticipated by 2020, reflecting the IoT's explosive growth over the previous ten years. [1].

One of the most difficult tasks for email service providers and users alike is identifying spam and non-spam messages. By getting users' attention with annoying messages, spammers attempt to distribute false information. . In order to locate the extreme values outside of the defined range, DBSCAN and Isolation Forest are utilised. The most useful features are chosen using the Heatmap, Recursive Feature Elimination, and Chi-Square feature selection procedures [2].

Motivated from these issues, in this paper, It is suggested to use the Cognitive Spammer Framework (CSF) to detect web spam. In addition to machine learning classifiers, fuzzy rule-based classifiers are used by CSF to identify web spam. The quality score of the website is generated by each classifier.

In order to create a single score that forecasts the spamicity of the web page, these quality scores are then combined. In CSF, the fuzzy voting approach is employed for ensembling [3]. The purpose of the next, i.e., the capability of an IoT network to resist to possible attacks by malicious agent that potentially could infect large areas of the network, spamming unreliable information and / or assuming unfair behaviors. In this sense, social resilience is devoted to face malicious activities of software agents in their social interactions, and do not deal with the correct working of the sensors and other information devices.

In this situation, using a reputation model to create local communities of agents based on their social skills may be a workable and productive approach.

II. LITERATURE SURVEY

A. Makkar et al.[1] suggest securing IoT devices by applying machine learning to identify spam. Spam Detection in IoT using Machine Learning framework is suggested to accomplish this goal. In this approach, a large number of input feature sets are used to evaluate five ML models using a variety of metrics. Each model uses the enhanced input attributes to calculate a spam score. This rating illustrates an IoT device's dependability based on a number of factors. The REFIT Smart Home data collection is utilised to verify the suggested method. In comparison to other current systems, the findings collected demonstrate the effectiveness of the proposed method.

F. Hossain et al.,[2] presents model based on the machine learning and deep learning to establish a comparative analysis. Multinomial Naïve Bayes (MNB), Random Forest (RF), K-Nearest Neighbor (KNN), Gradient Boosting (GB) are used to introduce ensemble method in machine learning implementation. In terms of accuracy and overhead produced, A. Makkar et al.'s [3] presentation of the WEBSPAM-UK 2007 dataset. From the results, it has been shown that CSF increases accuracy by 97.3%, which is relatively high when compared to other ways that have been described in the literature.

ResIoT is a framework proposed by G. Fortino et al. [4] for agents functioning in an IoT environment, where the establishment of communities for collaborative purposes is carried out on the basis of agent reputation. In order to test our strategy, we ran an experimental campaign using a simulated framework. This allowed us to confirm that, using our strategy, devices do not have any economic incentive to engage in deceptive behaviours. Further testing has revealed that our method is capable of identifying the types of active agents in systems (honest and malicious), with a detection accuracy of at least 11% compared to the best competitor tested and highlighting a high resilience with regard to some malicious activities.

Two representation approaches for graph-based datasets on social interaction are proposed by K. A. Al-Thelaya et al. [5].

The interactions and relationships between users are primarily used to construct the representation models. The development of the first model relies on graph-based analysis, whereas the development of the second model relies on the sequential processing of user interactions. We draw the conclusion that the two representation models exhibit good spam detection accuracy based on the trials that were done. However, compared to models for processing interaction sequences, graph-based analysis models yield accuracy levels that are higher.

A technique based on Wasserstein Generative Adversarial Network (WGAN) is suggested by J. Zhang et al. [7] to create malicious PDF files that resemble benign ones and can avoid the identification of malicious files. The experimental findings demonstrate that our method's adversarial examples can completely avoid the PDF classifier's PDFrate. We also evaluate how well they work with other classifiers, and the results demonstrate that our suggested approach is capable of dodging the detection of various machine learning techniques, including Support Vector Machine (SVM), Linear Regression, Decision Tree, and Random Forest.

It is suggested in a webpage filtering system by A. Makkar et al. [8] that spam web pages be automatically identified. The ranking module of search engines first detects spam websites before processing them. For the proposed system to be validated, the machine learning model, or decision tree, is used. The accuracy of the model is increased to 98.2% using the tenfold cross validation method. In the Cognitive Internet of Things (CIoT) environment, the results collected show that the suggested strategy has the ability to prevent spam web pages.

Without choosing any characteristics, A. K. Singh et al.[9] apply each classifier to the dataset in order to experiment with it and evaluate the results. Next, we use the best first feature selection algorithm and a variety of classification techniques to choose the desired features. When we used the feature selection technique in the experiment, we discovered that the accuracy had increased.

To give the reader a brief introduction to a thorough comprehension of the pertinent topics, T. Lange et al.,[10] review the evolution, trends, and mitigations of botnets and offer relevant examples and studies.

Without depending on fluid and shaky relationships, T. Qiu et al.'s[11] method for identifying spammers is intelligent. Each user node is assigned to a class during the model generation process in SIGMM, which integrates the presentation of data. Using a mobile network dataset from a cloud server, we compare the SIGMM with the reality mining algorithm and hybrid fuzzy c-means (FCM) clustering technique in order to validate it.

According to the simulation results, SIGMM performs better than these earlier systems in terms of recall, precision, and time complexity.

Kumar, G., et al.,[12] In order to express our opinions on the many topics that arise in our daily lives, social networking is quite vital. As a result, new channels of communication for the masses to express their ideas were opened. The information from these sites can be highly beneficial for analytical purposes.

- Trust modeling most of the current techniques for noise and spam reduction focus only on textual tag processing and user profile analysis while audio and visual content features of multimedia content can also provide useful information about the relevance of the content and content tag relation. In future challenge could be to combine multimedia content analysis with the conventional tag processing and user profile analysis.

III. Conclusion

In order to prevent IoT devices from gaining access to various services, the attackers can flood the target database with erroneous queries. Bots are the term used to describe these malicious queries sent by an IoT network of devices. DDoS might use up all of the resources that the service provider has available. It has the power to deny access to the network resource and to prohibit legitimate users. These are the assaults that have been made against IoT devices' physical layer.

REFERENCES

[1] A. Makkar, S. Garg, N. Kumar, M. S. Hossain, A. Ghoneim and M. Alrashoud, "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning," in IEEE Transactions on Industrial Informatics, vol. 17, no. 2, pp. 903-912, Feb. 2021, doi: 10.1109/TII.2020.2968927.

[2] F. Hossain, M. N. Uddin and R. K. Halder, "Analysis of Optimized Machine Learning and Deep Learning Techniques for Spam Detection," 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-7, doi: 10.1109/IEMTRONICS52119.2021.9422508.

[3] A. Makkar, U. Ghosh, P. K. Sharma and A. Javed, "A Fuzzy-based approach to Enhance Cyber Defence Security for Next-generation IoT," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3053326.

[4] G. Fortino, F. Messina, D. Rosaci and G. M. L. Sarne, "ResIoT: An IoT social framework resilient to malicious activities," in IEEE/CAA Journal of Automatica Sinica, vol. 7, no. 5, pp. 1263-1278, September 2020, doi: 10.1109/JAS.2020.1003330.

[5] K. A. Al-Thelaya, T. S. Al-Nethary and E. Y. Ramadan, "Social Networks Spam Detection Using Graph-Based Features Analysis and Sequence of Interactions Between Users," 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020, pp. 206-211, doi: 10.1109/ICIoT48696.2020.9089509.

[6] T. Y. Ho, W. Chen, M. Sun and C. Huang, "Visualizing the Malicious of Your Network Traffic by Explained Deep Learning," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 687-692, doi: 10.1109/ICAIIC48513.2020.9065247.

[7] J. Zhang, Q. Yan and M. Wang, "Evasion Attacks Based on Wasserstein Generative Adversarial Network," 2019 Computing, Communications and IoT Applications (ComComAp), 2019, pp. 454-459, doi: 10.1109/ComComAp46287.2019.9018647.

[8] A. Makkar, N. Kumar and M. Guizani, "The Power of AI in IoT : Cognitive IoT-based Scheme for Web Spam Detection," 2019 IEEE Symposium Series on Computational Intelligence (SSCI), 2019, pp. 3132-3138, doi: 10.1109/SSCI44817.2019.9002885.

[9] A. K. Singh, S. Bhushan and S. Vij, "Filtering spam messages and mails using fuzzy C means algorithm," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 2019, pp. 1-5, doi: 10.1109/IoT-SIU.2019.8777483.

[10] T. Lange and H. Kettani, "On Security Threats of Botnets to Cyber Systems," 2019 6th International Conference on Signal Processing and Integrated Networks (SPIN), 2019, pp. 176-183, doi: 10.1109/SPIN.2019.8711780.

[11] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah and B. Chen, "SIGMM: A Novel Machine Learning Algorithm for Spammer Identification in Industrial Mobile Cloud Computing," in IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2349-2359, April 2019, doi: 10.1109/TII.2018.2799907.

[12] G. Kumar and V. Rishiwal, "Statistical Analysis of Tweeter Data Using Language Model With KLD," 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519938.