JCST Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7641971

ANALYSIS OF SPAM IDENTIFICATION USING ARTIFICIAL INTELLIGENCE

Vijay kumar[1], Pratik Ranjan[2], Abha kumari[3], Raj Anwit[4]
[1,2,3] Assistant Professor, Motihari College of Engineering, Motihari
[4] Assistant Professor, Bhagalpur College of engineering, Bhagalpur

Abstract— There has been a correlation between security concerns and the rise of the artificial intelligence industry. Given its propensity to mine huge data for insights, In the domains of spam, machine learning has become widely used, fraud, and malicious file identification. Malicious attackers, on the other hand, have a strong incentive to avoid these techniques. Attackers are limited to using a "black box" assault because they don't know the exact details of the machine type. This study presents an overview of machine learning-based spam detection techniques for Internet of Things devices.

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

INTRODUCTION

With millions consisting of wired or wirelessly connected sensors and actuators that transmit data— the Internet of Things (IoT) is a network of interconnected objects. With over By 2020, there will likely be 25 billion connected gadgets. the Internet of Things has evolved quickly during the last ten years. In the coming years, These devices will generate many times as much data as they release. Many modalities and a large amount of data are generated by IoT devices differing data quality, which is determined by the speed of the data With regard to positional and temporal dependence, in addition to providing a higher volume. Computer learning (ML) techniques can be very helpful in this kind of setting in terms of Biotechnology-oriented permission and security, in addition to anomaly detection to improve IoT device security and usability. Nonetheless, learning algorithms are widely used by hackers to take advantage of security holes in intelligent Internet of Things systems [1].

Differentiating between two types of spam: emails is one of the trickiest problems for users and email service providers alike. Spammers attempt to disseminate false information by grabbing users' attention with obnoxious messages. Although a number of Spam detection algorithms have been developed put forth and evaluated in the past, the accuracy data indicates that more research in this area is required to obtain higher precision, shorter instruction times, and lower error rates. We have presented a model in this study effort that divides emails were categorised as spam and ham. To determine which excessive figures of fall outside of the designated range, DBSCAN and Isolation Forest are employed. The effective features are chosen using Chi-Square feature selection, Recursive Feature Elimination, and Heatmap methods [2].

The IoT networks of the future generation (Nx-IoT) are powered by the intelligence of sensing and computing since the Cognitive Internet of Things (CIoT) has been developed alongside the Internet of Things in the present era. In CIoT, With data scientists, there are found a plethora of methods for deriving understanding from data processing. After successfully completing this task, the data moves on to be processed further. One of the primary reasons of assaults on IoT is web spam. devices, which lead to their failure. A method that can identify It seems vital to stop online spam before it enters a gadget. In this paper, a proposed cognitive spammer framework (CSF) for web spam detection is constructed in response to these problems. Fuzzy rule-based classifiers and machine learning CSF uses classifiers to determine which internet spam is which. Every classifier creates a quality score for the webpage.

The web page's spam city is predicted by combining these quality values to get a single score. Fuzzy voting is the method used for ensembling in CSF [3]. The next generation of the internet of things, or IoT, aims to provide users with a wide range of services through highly sensitive, intelligent gadgets that can reason and act in real time. The potential to use agents' social disposition to facilitate between machines (M2M) interaction among intelligent entities is made possible through the fusion of multi-agent systems (MAS) and the Internet of Things. But choosing trustworthy collaborators in a federated and mobile environment is challenging, particularly when it comes to the almost total lack of device dependability. The above-discussed problems can be summed up by thinking back to the widely recognised idea of social adaptability within Internet of Things systems, which refers to an IoT network's ability to withstand potential harmful agent attacks that have the ability to spam faulty information, take unfair advantage of people, or infect significant areas of the network behaviours. In this way, social resilience does not concern itself with the proper operation of sensors and other information devices, but rather with fending off the malevolent behaviours of software agents in their interpersonal communications. Using a reputation model in this context can be a workable and efficient way to group agents into local communities according to their interpersonal skills.

LITERATURE SURVEY

A. Makkar et al.'s [1] proposal for IoT device security makes use of machine intelligence to detect spam. The proposal for Spam Detection in IoT using Machine Learning framework aims to accomplish this goal. Five machine learning models are assessed in this framework taking advantage of a variety of input feature sets and different metrics. Every model takes into account the refined input attributes in order to calculate a spam point total. How dependable an IoT gadget is shown by this score across a range of criteria. This technique is verified by means of REFIT Smart Home data collection. The outcomes demonstrate the suggested scheme's efficacy when compared to other current systems.

F. Hossain et al.,[2] A comparison study is established by the approach presented by that is based on machine learning and deep learning. Ensemble methods are introduced in machine learning implementations using Gradient Boosting (GB), Random Forest (RF), K-Nearest Neighbour (KNN), and Multinomial Naïve Bayes (MNB) systems. When multiple classifiers' output needs to be combined, an ensemble method is developed. Comparing ensemble approaches to single classifiers allows for higher prediction accuracy. We found that our suggested model has an accuracy of 100%, AUC=100, MSE error = 0 and RMSE error = 0 for machine learning implementation and accuracy of 99%, loss value= 0.0165 for implementation of deep learning using a basic dataset of email spam gathered extracted from the machine learning repository at UCI.

A. Makkar et al.,[3] gives an accurate and overhead-generated display of the dataset from WEBSPAM-UK 2007. As demonstrated from the data that CSF increases accuracy by 97.3%, which is a relatively large improvement when compared to other ways that have been documented in research.

G. Fortino and others, [4] provide a framework, known as ResIoT, for agents functioning in an IoT context where communities are formed for cooperative purposes based on agent reputation. We conducted a trial campaign to evaluate our method in a simulated environment. This made it possible for us to verify that our plan eliminates any economic convenience for devices to engage in false behaviours. Furthermore, in comparison to the top-tested rival, our approach's accuracy in identifying the honest and malicious the characteristics of the systems' active agents is at least 11%, indicating a high level of resilience against some malicious activities. These experimental results support our approach.

K. A. Al-Thelaya and others, [5] propose two approaches of representation for graph-based datasets on social interaction. The primary basis for developing the representation models is the analysis of user relationships and interactions. Based on graph-based analysis, the first model differs from the second, which is based on the sequential processing of user interactions. We draw the conclusion that both representation models exhibit great accuracy in detecting spam, based on the conducted trials. However, compared to interaction sequences processing models, An analytical model based on graphs yield higher levels of accuracy.

Ho, T. Y. and colleagues, [6] pay attention to the traffic behaviour and solely take into account the characteristics of the source and destination IPs, connection timestamps, and connection quantity. Using deep learning in this study paradigm is applied to tackle the problem of complex network traffic. A modified version of VGG16 is proposed to analyse traffic flow aspects. In conclusion, the learning model approach presented in this research offers a way to facilitate further explanation of traffic behaviour.

Zhang, J. and others, [7] suggests a technique to create malicious PDF files that resemble innocuous ones and can avoid the malicious file detection system. This technique is based on an adversarial network that is generative and Wasserstein (WGAN). The experimental results show that hostile examples of our strategy are able to avoid the PDF classifier-PDFrate of 100%. Additionally, we evaluate how well they perform in various classifiers. The findings demonstrate that our suggested strategy is capable of eluding the classification algorithms of several machine learning methods, including Support Vector Machine (SVM), Linear Regression, Decision Tree, and Random Forest.

A. Makkar et al.,[8] An automatic webpage filtering system that identifies spam websites is presented. Search engine ranking modules finds the spam webpages before it processes them. The suggested system is validated using An example of a machine learning decision tree model. To increase the model's accuracy to 98.2%, the tenfold cross validation procedure is employed. The outcomes show that the suggested strategy can effectively block spam websites in an environment of the Cognitive Internet of Things (CIoT).

A. K. Singh et al.,[9] Use the dataset as an experiment and analyse the results by applying each classifier without specifying any characteristics. In order to choose the desired features, we then use different classification methods and the best first feature selection algorithm. After implementing a feature selection method during the trial, we discovered that the accuracy had increased.

T. Lange et al.,[10] give a summary of the development, trends, and mitigations of botnets along with relevant studies and examples to give the reader a fast overview among the current issues.

T. Qiu et al.,[11] allows for the intelligent identification of spammers without depending on flimsy and unstable connections. SIGMM integrates data presentation, with each user node being assigned to a class during the model's creation. We verify the SIGMM by contrasting it with the clustering using hybrid fuzzy c-means (FCM) method and reality mining technique with a dataset from a mobile network sourced from a cloud server. The outcomes of the simulation demonstrate that SIGMM performs better regarding recall, accuracy, and temporal complexity than these earlier systems.

G. Kumar et al.,[12] Social networking is essential component of our daily lives since it allows us to express our opinions on a wide range of problems. because it made it possible for the general public to communicate and exchange ideas. For analytical purposes, the data from these websites might be quite helpful.

CHALLENGES

There are some challenges to these techniques. Some of them are highlighted below:

- In trust modeling system user’s trust tends to vary over time according to the user’s experience and involvement of social networks.

Only a few approaches deals with the dynamics of trust by distinguishing between recent and old tags. Future work considering dynamics of trust would lead to better modeling in real world application.

- Most of the existing approaches based on text information assuming monolingual environment.

- However social network services are used by people from various countries, so various languages simultaneously appears in tags and comment. In such cases some text information may be regarded as wrong or considered as spam due to language spam. Therefore incorporating multilinguist in trust modelling would solve this problem.

It is observed that interaction across social network become popular. For e.g. users can use their Facebook accounts to log in some other social network services. Thus future challenge is to investigate how trust model across domains can be effectively connected and shared.

- 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.

CONCLUSION

To prevent IoT devices from accessing different services, the assailants are able to overwhelm the target database with unsolicited requests. Bots are the term used to describe these fraudulent requests generated by an IoT device network. DDoS has the ability to deplete every resource that the service provider offers. It can prevent prohibit authorised users and restrict access to the network resource. These are the physical layer attacks on Internet of Things devices.

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. 2020, 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," 2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2020, 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.