International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 11, Issue 07, July 2022)

Machine Learning for Detection of SPAM in the IOT Network : A Review

Sarfaraj Alam[1], Sonal Chaudhary[2]

Mtech Scholar[1], Associate Professor[2], Department of Computer Science & Engineering, All Saints' College of Technology, Bhopal, Madhya Pradesh, India

***Abstract*— Security issues have been accompanied by the development of the artificial intelligence industry. Machine learning has been widely used for fraud detection, spam detection, and malicious file detection, since it has the ability to dig the value of big data. However, for malicious attackers, there is a strong motivation to evade such algorithms. Because attackers do not know the specific parameters of the machine model, they can only carry out a black box attack. This paper presents the review of spam detection techniques for IoT devices using machine learning.**

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

I. INTRODUCTION

The Internet of Things (IoT) is a group of millions of devices having sensors and actuators linked over wired or wireless channel for data transmission. IoT has grown rapidly over the past decade with more than 25 billion devices expected to be connected by 2020. The volume of data released from these devices will increase many-fold in the years to come. In addition to an increased volume, the IoT devices produces a large amount of data with a number of different modalities having varying data quality defined by its speed in terms of time and position dependency. In such an environment, machine learning (ML) algorithms can play an important role in ensuring security and authorization based on biotechnology, anomalous detection to improve the usability, and security of IoT systems. On the other hand, attackers often view learning algorithms to exploit the vulnerabilities in smart IoT-based systems [1].

Spam and non-spam email identification are one of the most challenging tasks for both email service providers and consumers. The spammers try to spread misleading facts through irritating messages by attracting user's attention. Several spam identification-models have previously been proposed and tested but the recorded accuracy has shown that further work in this direction is needed to achieve improved accuracy, low training time, and less error rate. In this research work, we have proposed a model that classifies the e-mail into spam and ham. DBSCAN and Isolation Forest are used to identify the extreme values outside of the specific range.

Heatmap, Recursive Feature Elimination, and Chi-Square feature selection techniques are used to select the effective features [2].

In modern era, Cognitive Internet of Things (CIoT) in conjunction with IoT evolves which provides the intelligence power of sensing and computation for next-generation IoT (Nx-IoT) networks. The data scientists have discovered a large amount of techniques for knowledge discovery from processed data in CIoT. This task is accomplished successfully and data proceeds for further processing. The major cause for the failure of IoT devices is due to the attacks, in which web spam is more prominent. There seems a requirement of a technique which can detect the web spam before it enters into a device. Motivated from these issues, in this paper, Cognitive spammer framework (CSF) for web spam detection is proposed. CSF detects the web spam by fuzzy rule based classifiers along with machine learning classifiers. Each classifier produces the quality score of the webpage.

These quality scores are then ensembled to generate a single score, which predicts the spamicity of the web page. For ensembling, fuzzy voting approach is used in CSF [3]. The purpose of the next internet of things (IoT) is that of making available myriad of services to people by high sensing intelligent devices capable of reasoning and real time acting. The convergence of IoT and multi-agent systems (MAS) provides the opportunity to benefit from the social attitude of agents in order to perform machine-to-machine (M2M) cooperation among smart entities. However, the selection of reliable partners for cooperation represents a hard task in a mobile and federated context, especially because the trustworthiness of devices is largely unreferenced. The issues discussed above can be synthesized by recalling the well known concept of social resilience in IoT systems, 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 setting, the use of a reputation model can be a practicable and effective solution to form local communities of agents on the basis of their social capabilities.

II. Literature Survey

A. Makkar et al., [1] propose the security of the IoT devices by detecting spam using ML. To achieve this objective, Spam Detection in IoT using Machine Learning framework is proposed. In this framework, five ML models are evaluated using various metrics with a large collection of inputs features sets. Each model computes a spam score by considering the refined input features. This score depicts the trustworthiness of IoT device under various parameters. REFIT Smart Home data set is used for the validation of proposed technique. The results obtained prove the effectiveness of the proposed scheme in comparison to the other existing schemes.

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. An ensemble method is constructed to combine multiple classifiers' output. The ensemble methods allow producing better prediction accuracy compared to a single classifier. Our proposed model obtained 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 deep learning implementation based on an email spam base dataset collected from the UCI machine learning repository.

A. Makkar et al., [3] presents the dataset WEBSPAM-UK 2007 with respect to accuracy and overhead generated. From the results obtained, it has been demonstrated that CSF improves the accuracy by 97.3%, which is comparatively high in comparison to the other existing approaches in literature.

G. Fortino et al., [4] propose a framework for agents operating in an IoT environment, called ResIoT, where the formation of communities for collaborative purposes is performed on the basis of agent reputation. In order to validate our approach, we performed an experimental campaign by means of a simulated framework, which allowed us to verify that, by our approach, devices have not any economic convenience to perform misleading behaviors.

Moreover, further experimental results have shown that our approach is able to detect the nature of the active agents in the systems (i.e., honest and malicious) , with an accuracy of not less than 11 % compared to the best competitor tested and highlighting a high resilience with respect to some malicious activities.

K. A. Al-Thelaya et al., [5] suggest two representation models for social interaction's graph-based datasets. The representation models are mainly developed based on analyzing interactions and relations between users. The first model is developed based on graph-based analysis, while the other one is developed based on sequential processing of user interactions. Based on the conducted experiments, we conclude that the two representation models show high spam detection accuracy. However, graph-based analysis models produce higher accuracy levels compared to those produced by interaction sequences processing models.

T. Y. Ho et al., [6] focus on the traffic behavior that we only consider the features of source IP, destination IP, timestamp of connection, and quantity of connection. To conquer the black box of complicated network traffic, this work applies the deep learning paradigm and proposes the variant version of VGG16 to examine the features within traffic flow. Finally, this paper proposes a method to support more explanation on traffic behavior with learning model.

J. Zhang et al., [7] proposes a method based on Wasserstein Generative Adversarial Network(WGAN) to generate malicious PDF files which are similar to benign ones and can evade the malicious file detection system. The experimental results show that the adversarial examples generated by our method can evade the PDF classifier-PDFrate of 100%. We also test their performance in different classifiers and the results show that our proposed method can evade the classifiers of different machine learning algorithms such as Support Vector Machine (SVM), Linear Regression, Decision Tree, Random Forest.

A. Makkar et al., [8] presents webpage filtering algorithm is proposed which automatically detects the spam web pages. The spam webpages are detected before these are processed by the ranking module of search engines. The machine learning model, i.e., decision tree is used for the validation of the proposed scheme. The tenfold cross validation approach is used to improve the accuracy of model, i.e., 98.2%. The results obtained demonstrate that the proposed scheme has the power of preventing the spam web pages in Cognitive Internet of Things (CIoT) environment.

A. K. Singh et al., [9] apply each classifier without selecting any features in order to experiment on the dataset and examine the outcome. Next, to select the desired features we apply best first feature selection algorithm and apply various algorithms for classification. We found that the accuracy has improved when we applied feature selection process in the experimentation.

T. Lange et al., [10] present a review on botnet evolution, trends and mitigations, and offer related examples and research to provide the reader with quick access to a broad understanding of the issues at hand.

T. Qiu et al., [11] provides intelligent identification of spammers without relying on flexible and unreliable relationships. SIGMM combines the presentation of data, where each user node is classified into one class in the construction process of the model. We validate the SIGMM by comparing it with the reality mining algorithm and hybrid fuzzy c-means (FCM) clustering algorithm using a mobile network dataset from a cloud server. Simulation results show that SIGMM outperforms these previous schemes in terms of recall, precision, and time complexity.

G. Kumar et al., [12] Social Networking plays a very important part in our day to day life to share our views on various issues those arise. As it opened new means of communication between masses to share their thoughts. The data from these sites can be very useful for the purpose of analysis.

R. Mishra et. al [13] IoT, an word form for the internet of Things. Within the recent era of rising Science and Technology nearly most of the items are automated. Operating within the smart and auto switched method. In one click or in one touch through different sensors, innovative analysis and large computing with new paradigms.

V. Rajpoot et. al [14] Sentiment analysis is the investigation of feelings and conclusions from any type of text. It is additionally named as assessment. This is extremely helpful to communicate the assessment of the gathering person.

V. Rajpoot et. al [15] The Improved tree seed algorithm and K-Nearest Neighbor (ITSA-KNN) method suggested selecting features to improve the intrusion detection identification performance in this study.

V. Rajpoot et. al [16] Machine learning encourages many real solutions that optimise resource use and increase the network's lifespan in sensor networks.

III. 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 multilinguism in trust modelingwould 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.

IV. Conclusion

The attackers can flood the target database with unwanted requests to stop IoT devices from having access to various services. These malicious requests produced by a network of IoT devices are commonly known as bots. DDoS can exhaust all the resources provided by the service provider. It can block authentic users and can make the network resource unavailable. These are the attacks imposed at the physical layer of IoT device.

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.

[13] R. Mishra, M. Gupta, V. Rajpoot "An Iot Based Environmental Strategic Solution For Fire And Air Pollution Using Cloud Computing Platform" 2021 5th International Conference on Information Systems and Computer Networks (ISCON) DOI: 10.1109/ISCON52037.2021.9702349

[14] V Rajpoot, R Agrawal, A Chaturvedi, K Goyal "An Empirical Study of Sentiment Analysis on Movie Review using Machine Learning based Classification Approach" 2021 5th International Conference on Information Systems and Computer Networks (ISCON) 2021 DOI: 10.1109/ISCON52037.2021.9702471

[15] V Rajpoot, R Agrawal ITSA-KNN: Feature Selection Model Based on Improved Tree-Seed Algorithm and K-Nearest Neighbor for Network Intrusion Detection Advances in Data and Information Sciences, 2022 https://doi.org/10.1007/978-981-16-5689-7_1

[16] V Rajpoot, L Garg, MZ Alam, V Parashar, P Tapashetti Analysis of machine learning based LEACH robust routing in the Edge Computing systems Computers & Electrical Engineering, 2021 https://doi.org/10.1016/j.compeleceng.2021.107574