Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

A NOVEL APPROACH FOR EFFICIENT SPAM DETECTION ON IOT DEVICES USING MACHINE LEARNING

RAMAKRISHNA NALLIBOYINA, Assistant. Professor , Department of Computer Science & Engineering, RGUKT NUZVID-521201, Eluru Dt. (A.P).
SRAVAN KUMAR KALAPALA, Assistant. Professor, Department of Computer Science & Engineering, RGUKT NUZVID-521201, Eluru Dt. (A.P).

Abstract —in this paper, A quality of these data will fluctuate depending on the time and location, which is represented by their speed. One can't depict IOT without Machine Learning(ML) considering the way that it has the greater part of the significant highlights like security, simple to utilize, reliable,as well as fit in making and utilizing a Smart gadget. It's certainly not astonishing to say that another progression might be assaulted. To accomplish information confirmation and fix security issues in IOT. This paper proposed, Supervised ML frameworks which is utilized for mark the relationship for fruitful recognization of DOS assaults, Intrusion, Spoofing assault, Malware, etc ML models assess utilizing different assessments with a monstrous assortment of Input highlight sets. The proposed method uses the impressive REFIT housing data set. The outcomes gained shows the fittingness, proposed plot then again with the current plans.

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 are expected to be connected by 2021. 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 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. The definition of email spam is vague because everyone has an opinion about it. At the moment, everyone's attention is drawn to email spam. In most cases, email spam consists of one-off messages sent in bulk by people you don't know. (The term spam comes from a Monty Python sketch, in which a Hormel canned beef item had a lot of annoying emphases.) While the term "spam" is said to have originally been coined in 1978 to refer

to unsolicited email, it exploded in popularity in the mid-1990s, as we began to become more widely known outside of academic and research circles. The development expenditure trick is a well-known example, in which a client receives an email with an offer that should result in a prize.In today's technological age, the dodger/spammer tells a scenario in which the unlucky victim requires immediate financial assistance so that the fraudster can amass a much larger sum of money, which they would subsequently share. When the unfortunate victim completes the instalment, the fraudster will either make a profit or avoid communication.

LITERATURE SURVEY

AUTHORS: W. Kim, O.-R. Jeong, C. Kim, and J. So The Internet and Web technologies have originally been developed assuming an ideal world where all users are honorable. However, the dark side has emerged and bedeviled the world. This includes spam, malware, hacking, phishing, denial of service attacks, click fraud, invasion of privacy, defamation, frauds, violation of digital property rights, etc. The responses to the dark side of the Internet have included technologies, legislation, law enforcement, litigation, public awareness efforts, etc. In this paper, we explore and provide taxonomies of the causes and costs of the attacks, and types of responses to the attacks.

AUTHORS: Eirini Anthi - The proposed paper, depict the mystical events of generting an Intrusion Detection System for IOT, that uses ML theory and will do satisfactorily perceiving community investigating assessment as well as obvious kinds of assaults.

AUTHORS: Aaisha Makkar - In this particular, cognitive spammer framework(CSF) for web unsolicited info recognition is applied. CSF detects the net unsolicited info by fuzzy rule based classifieds together with ML classifiers. each classifier creates the quality rating would be the outfits to create one score, and that predicts the spamicity of web page. for gathering, fuzzy voting strategy is utilized in CSF. The tests had been conducted utilizing regular dataset as for accuracy and overhead created. By the outcomes got, it's been exhibited that CSF improves the accuracy by 97.3 % and that is fairly high to the subsequent existing methodologies

PROPOSED METHOD

The proposed scheme of spam detection in IOT is validated using machine learning model. An algorithm is proposed to compute the spamicity score of the model which is then used for detection and intelligent

decision making. Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics. To protect the IoT devices from producing the malicious information, the web spam detectionϖ is targeted in this proposal. We have considered the machine learning algorithm for the detection of spam from the IoT devices. The dataset used in the experiments, contains the data recorded for the span of eighteenϖ months. For better results and accuracy, we have considered the data of one month. Considering the fact, the climate is the important parameter for the working of IoT device, the month with maximum variations has been taken into the consideration.

ADVANTAGES OF PROPOSED SYSTEM:

1.Machine learning techniques help to build protocols for lightweight access control to saveϖ energy and extend the IoT systems lifetime.

2.The efficiency IoT data increases, if stored, processed and retrieved in an efficient manner.ϖ This proposal aims to reduce the occurrence of spam from these devices.

METHODOLOGY

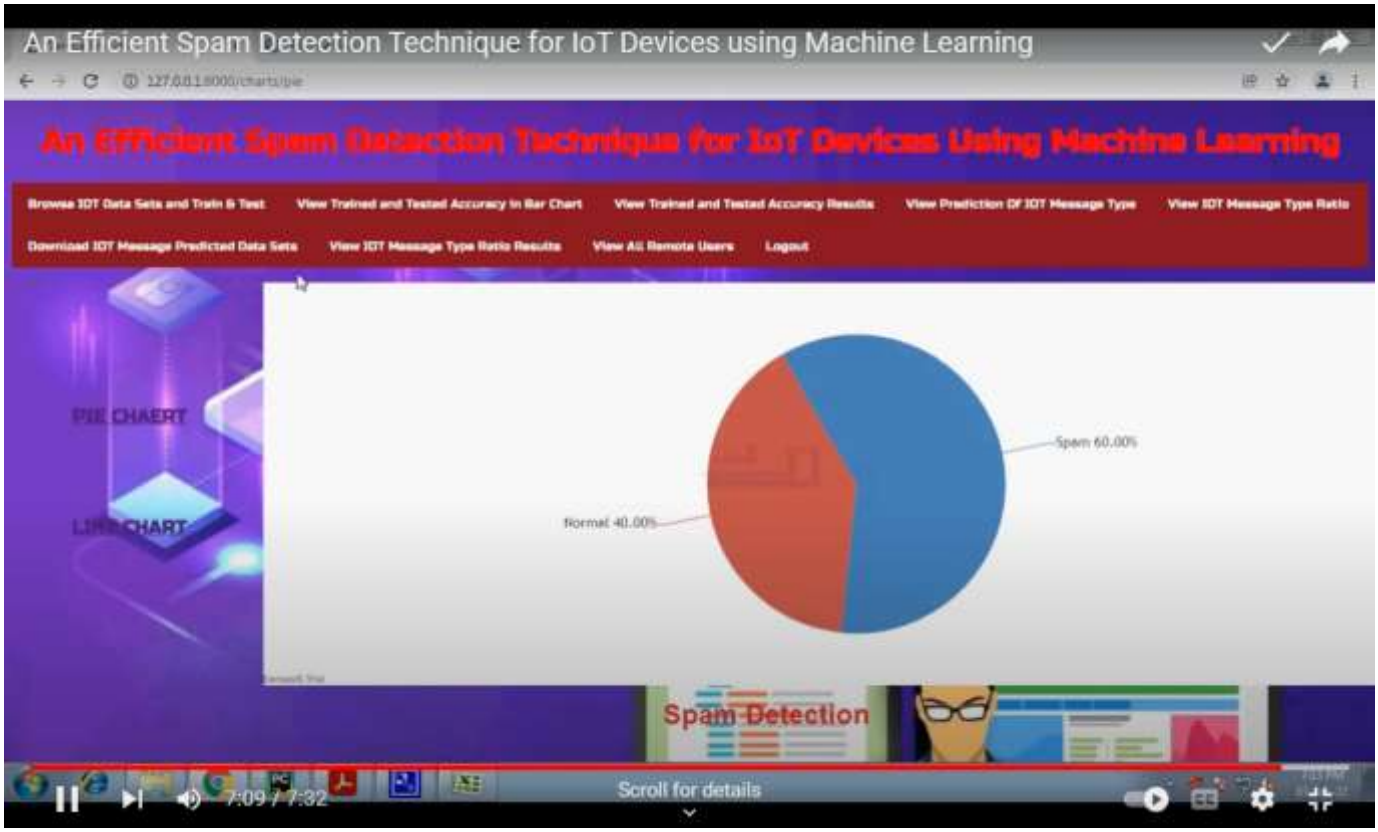
SVM(support vector machine) is the flexible supervised ML procedure. It is mainly useful in regression and classification challenges but primarily for classification purposes. They have an extra-ordinary ability to handle multiple continuous and categorial variables. Comparing with other algorithms they have unique way of representing and implementing. They perform classification by selecting a hyperplane which maximizes the margin among two classes. The vector which describes the hyperplane is support vector. This algorithm picks the acute vectors that assist in increasing hyperplane. These extreme instances called support vectors, hence consequently called the procedure as support vector mechine.

Data Collection: This is the first real step towards the real development of a machine learning model, collecting data. This is a critical step that will cascade in how good the model will be, the more and better data that we get, the better our model will perform. There are several techniques to collect the data, like web scraping, manual interventions and etc.

SAMPLE RESULTS

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, August : 2023



CONCLUSION

In this paper, spam parameters of IoT devices using machine learning models. The IoT dataset used for experiments, is pre-processed by using feature engineering procedure. By experimenting the framework with machine learning models, each IoT appliance is awarded with a spam score. This refines the conditions to be taken for successful working of IoT devices in a smart home

References

[1]. Aaisha Makkar; Sahil Garg; Neeraj Kumar; M. Shamim Hossain; Ahmed Ghoneim; Mubarak Alrashoud "An Efficient Spam Detection Technique for IoT Devices Using Machine Learning " DOI : 10.1109/TII.2020.2968927.

[2]. Farooq Shaikh; Elias Bou-Harb; Jorge Crichigno; Nasir Ghani "A Machine Learning Model for Classifying Unsolicited IoT Devices by Observing Network Telescopes" DOI: 10.1109/IWCMC.2018.8450404.

[3]. Aaisha Makkar; Neeraj Kumar; Mohsen Guizani "The Power of AI in IoT: Cognitive IoTbased Scheme for Web Spam Detection" DOI: 10.1109/SSCI44817.2019.9002885.

[4] C. Zhang and R. Green, “Communication security in internet of thing: preventive measure and avoid ddos attack over iot network,” in Proceedings of the 18th Symposium on Communications & Networking. Society for Computer Simulation International, 2015, pp. 8–15.

[5] W. Kim, O.-R. Jeong, C. Kim, and J. So, “The dark side of the internet: Attacks, costs and responses,” Information systems, vol. 36, no. 3, pp. 675–705, 2011.

[6] H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for nfc applications,” IEEE Transactions on Consumer Electronics, vol. 59, no. 1, pp. 153–160, 2013.

[7]. H. Eun, H. Lee, and H. Oh, “Conditional privacy preserving security protocol for nfc applications,” IEEE Transactions on Consumer Electronics, vol. 59, no. 1, pp. 153–160, 2013.

[8]. R. V. Kulkarni and G. K. Venayagamoorthy, “Neural network based secure media access control protocol for wireless sensor networks,” in 2009 International Joint Conference on Neural Networks. IEEE, 2009, pp. 1680– 1687.

[9]. M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learning in wireless sensor networks: Algorithms, strategies, and applications,"IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1996–2018, 2014.

[10]. A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2015.

[11]. F. A. Narudin, A. Feizollah, N. B. Anuar, and A. Gani, "Evaluation of machine learning classifiers for mobile malware detection," Soft Computing, vol. 20, no. 1, pp. 343–357, 2016.

[12]. N. Sutta, Z. Liu, and X. Zhang, "A study of machine learningalgorithms on email spam classification," in Proceedings of the 35th International Conference, ISC High Performance 2020, vol. 69, pp. 170– 179,Frankfurt,Germa.

[13]. L. Xiao, Y. Li, X. Huang, and X. Du, "Cloud-based malware detection game for mobile devices with offloading," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2742–2750, 2017.

[14]. J. W. Branch, C. Giannella, B. Szymanski, R. Wolff, and H. Kargupta, "In-network outlier detection in wireless sensor networks," Knowledge and information systems, vol. 34, no. 1, pp. 23–54, 2013.

[15]. I. Jolliffe, Principal component analysis. Springer, 2011.

[16]. I. Guyon and A. Elisseeff, "An introduction to variable and feature selection," Journal of machine learning research, vol. 3, no. Mar, pp. 1157–1182, 2003.

[17]. L. Yu and H. Liu, "Feature selection for high-dimensional data: A fast correlation-based filter solution," in Proceedings of the 20th international conference on machine learning (ICML-03), 2003, pp. 856–863.

[18]. A. H. Sodhro, S. Pirbhulal, and V. H. C. de Albuquerque, "Artificial intelligence driven mechanism for edge computing based industrial applications," IEEE Transactions on Industrial Informatics, 2019.