SPAM DETECTION TECHNIQUE FOR IOT DEVICES USING MACHINE LEARNING

M.Praveena, M.Sc.(Computer Science) Lecturer, Department of Computer Science, Sri Durga Malleswara Siddhartha Mahila Kalasala, Vijayawada

D.Varalaxmi, M.Sc.,M.Tech(CSE) Lecturer, Department of Computer Science, Sri Durga Malleswara Siddhartha Mahila Kalasala, Vijayawada

ABSTRACT:

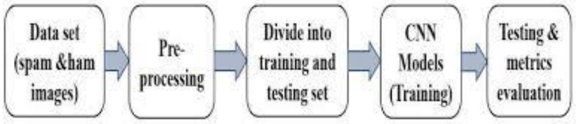
In This Paper review the volume of data released from these devices will increase manyfold in the years to come. In addition to an increased volume, the IoT devices produces a large amount of data with a number of different modalities having varying data quality defined by its speed in terms of time 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.

KEYWORDS: Spam Detection, IoT Devices,ML.

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 2020. Internet of Things (IOT) empowers combination, information analysis as well as implementation among these present reality protests regardless of their topographical areas. Execution of such organization management and control make security and insurance methodologies most extreme significant and testing in such a platform. IOT packages want to make certain facts safety to repair protection problems like interruptions, phishing attacks, DOS attacks, spam, malware and others. literature survey of machine learning (ML) and data mining (DM) methods for cyber analytics in support of intrusion detection. Short tutorial descriptions of each ML/DM method are provided. Based on the number of citations or the relevance of an emerging method, papers representing each method were identified, read, and summarized. Because data are so important in ML/DM approaches, some well-known cyber data sets used in ML/DM are described. The complexity of ML/DM algorithms is addressed, discussion of challenges for using ML/DM for cyber security is presented, and some recommendations on when to use a given method are provided.

DOI : 10.36893.DRSR.2021.V08I14.65-69


Data set (spam &ham images)
Pre-processing
Divide into training and testing set
CNN Models (Training)
Testing & metrics evaluation

PROBLEM STATEMENT

Denial of service (DDoS) attacks: 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 [3]. DDoS can exhaust all the resources provided by the service provider. It can block authentic users and can make the network resource unavailable.

RFID attacks: These are the attacks imposed at the physical layer of IoT device. This attack leads to loose the integrity of the device. Attackers attempt to modify the data either at the node storage or while it is in the

transmission within network. The common attacks possible at the sensor node are attacks on availability, attacks on authenticity, attacks on confidentiality, Cryptography keys brute-forcing [4]. The countermeasures to ensure prevention of such attacks includes password protection,

data encryption and restricted access control.

Internet attacks: The IoT device can stay connected with Internet to access various resources. The spammers who want to steal other systems information or want their target website to be visited continuously, use spamming techniques [5]. The common technique used for the same is Ad fraud. It generates the artificial clicks at a targeted website for monetary profit. Such practicing team is known as cyber criminals.

PROPOSED APPROACH

Detects the 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. In future, we are planning to consider the climatic and surrounding features of IoT device to make them more secure and trustworthy.

The Internet of Things is part of our everyday life, which applies to all aspects of human life; from smart phones and environmental sensors to smart devices used in the industry. Although the Internet of Things has many advantages, there are risks and dangers as well that need to be addressed. The information used and transmitted on Internet of Things contain important info about the daily lives of people, banking information, location and geographical information, environmental and medical information, together with many other sensitive data. Therefore, it is critical to identify and address the security issues and challenges of Internet of Things. In this article, considering the broad scope of this field and its literature, we are going to express some comprehensive information on security challenges of the Internet of Things.

LITERATURE SURVEY

AC Sarma, J Girão - Wireless personal communications, 2009 - Springer

There are two problem areas of the current Internet to be solved in Future Internet scenarios—security and putting the user back in control despite the move to the Internet of things. With this in mind, we address problems associated with the diversifying of the Internet towards an Internet of things, and with increased ways to be reachable, whether the user wants it or not, in the digital world. The paper presents two approaches to cope with the problem: The Identinet and a concept designated by the digital shadow.

J. Liu, Y. Xiao, and C. L. P. Chen. "Authentication and Access Control in the Internet of Things," In IEEE 32nd International Conference on Distributed Computing Systems Workshops, June 2012.

Due to the inherent vulnerabilities of the Internet, security and privacy issues should be considered and addressed before the Internet of Things is widely deployed. This paper mainly analyzes existing authentication and access control methods, and then, it designs a feasible one for the Internet of Things.

ALGORITHMS:

SVM: SVM is a supervised machine learning algorithm which can be used for classification or regression problems. It uses a technique called the kernel trick to transform your data and then based on these transformations it finds an optimal boundary between the possible outputs.

Step 1: There are number of images present in image database and first step is to extract the features from images present in database.

DOI : 10.36893.DRSR.2021.V08I14.65-69

Step 2: The performance of Context Based Image Processing Using Machine Learning Approaches is depend on shape, texture and color or other features of image. For this feature extraction CNN algorithm is used.

Step 3: The shape, texture and color information low level features of images are extracted. And in feature database these features are stored as feature vector.

Step 4: A query image is enters into the system. After extraction of query image features a feature vector is generated which is further compared with all vector stored in database.

Step 5: In high dimensional feature space firstly the image data is represented in terms of features and then images similarity is stored in the database which is further compared with query image. For the comparison of image features and query features SVM algorithm is used.

CONCLUSION

To protect the IoT devices from producing the malicious information, the web spam detection is targeted in this proposal. We have considered various machine learning algorithms for the detection of spam from the IoT devices. The target is to resolve the issues in the IoT devices deployed within home. But, the proposed methodology considers all the parameters of data engineering before validating it with machine learning models.

REFERENCES:

[1] Yu-Hao Hsu, Fuchun Joseph Lin, "Preventing Misuse of Duplicate Certificates in IoT/M2M Systems", *Computer Communication and Networks (ICCCN) 2017 26th International Conference on*, pp. 1-8, 2017.

[2] Kruthika Rathinavel, Manisa Pipattanasomporn, Murat Kuzlu, Saifur Rahman, "Security concerns and countermeasures in IoT-integrated smart buildings", *Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017 IEEE*, pp. 1-5, 2017.

[3] Se-Ra Oh, Young-Gab Kim, "Security Requirements Analysis for the IoT", *Platform Technology and Service (PlatCon) 2017 International Conference on*, pp. 1-6, 2017.

[4] Litun Patra, Udai Pratap Rao, "Internet of Things — Architecture applications security and other major challenges", *Computing for Sustainable Global Development (INDIACom) 2016 3rd International Conference on*, pp. 1201-1206, 2016.

DOI : 10.36893.DRSR.2021.V08I14.65-69

[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] 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.

[8] 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.

[9] 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.

[10] 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.

[11] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, “A system for denial-of-service attack detection based on multivariate correlation analysis,” IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 447–456, 2013.

[12] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, “Sinr-based dos attack on remote state estimation: A game-theoretic approach,” IEEE Transactions on Control of Network Systems, vol. 4, no. 3, pp. 632–642, 2016.

[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.