IJITCE

ISSN 2347- 3657

International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 12, Issue 3, 2024

An Efficient Spam Detection Technique for IoT Devices using Machine Learning

[1]P MOUNIKA, [2] V.DURGA BHAVANI

[1](Assistant Professor), **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

[2]MCA, scholar, **DANTULURI NARAYANA RAJU COLLEGE(A) PG COURSES, BHIMAVARAM ANDHRA PRADESH**

ABSTRACT

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. 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 toimprove 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. Motivated from these, in this paper, we propose the security of the IoT devices by detecting spam using machine learning. To achieve this objective, Spam Detection in IoT using Machine Learning framework is proposed. In this framework, five machine learning 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 dataset is

ISSN 2347–3657

Volume 12, Issue 3, 2024

used for the validation of proposed technique. The results obtained proves the effectiveness of the proposed scheme in comparison to the other existing schemes.

1.INTRODUCTION

Internet of Things (IoT) enables convergence and implementations between the real-world objects irrespective of their geographical locations. Implementation of such network management and control make privacy and protection strategies utmost important and challenging in such an environment. IoT applications need to protect data privacy to fix security issues such as intrusions, spoofing attacks, DoS attacks, DoS attacks, jamming, eavesdropping, spam, and malware. The safety measures of IoT devices depends upon the size and type of organization in which it is imposed.

The behavior of users forces the security gateways to cooperate. In other words, we can say that the location, nature, application of IoT devices decides the security measures [1]. For instance, the smart IoT security cameras in the smart organization can capture the different parameters for analysis and intelligent decision making [2]. The maximum care to be taken is with web based devices as maximum number of IoT devices are web dependent. It is common at the workplace that the IoT devices installed in an organization can be used to implement security and privacy features efficiently.

For example, wearable devices collect and send user's health data to a connected smartphone should prevent leakage of information to ensure privacy. It has been found in the market that 25-30% of working employees connect theirpersonal IoT devices with the organizational network. The expanding nature of IoT attracts both the audience, i.e., the users and the attackers. However, with the emergence of ML in various attacks scenarios, IoT devices choose a defensive strategy and decide the key parameters in the security protocols for trade-off between security, privacy and computation. This job is challenging as it is usually difficult for an IoT system with limited resources toestimate the current network and timely attack status.

Contributions Based upon the above discussions, following contributions are presented in this paper. 1) The proposed scheme of spam detection is validated using five different machine learning models. 2) An algorithm is proposed to compute the

ISSN 2347–3657

Volume 12, Issue 3, 2024

spam city score of each model which is then used for detection and intelligent decision making. 3) Based upon the spam city score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.B. Organization Rest of the paper is structured as follows. Section II discussed the related work. Section III illustrated the proposed scheme. Results are discussed and analyzed in Section IV. Finally, the paper is concluded in Section V.

2. EXISTING SYSTEM

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 lose 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.

NFC attacks: These attacks are mainly concerned with electronic payment frauds. The possible attacks are unencrypted traffic, Eavesdropping, and Tag modification. The solution for this problem is the conditional privacy protection. So, the attacker fails to create the same profile with the help of user's public key [6]. This model is based on random public keys by trusted service manager.

Disadvantages

ISSN 2347–3657

Volume 12, Issue 3, 2024

- In the existing work, the system is less effective due to lack of Spam Detection in IoT using Machine Learning framework.

- This system is less performance in which it is clear that Supervisedmachine learning techniques is absence.

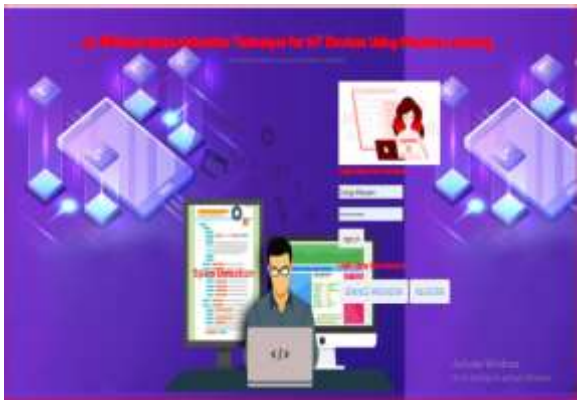
3. PROPOSED SYSTEM

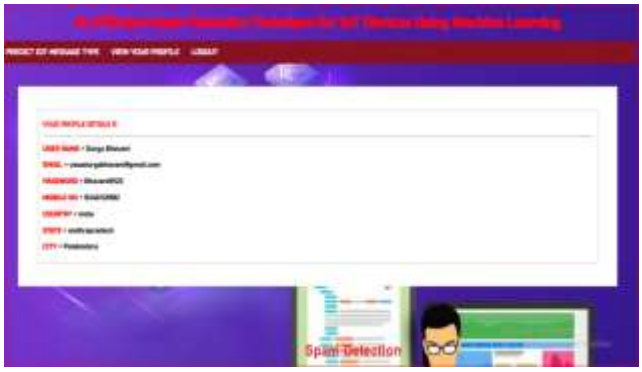
The digital world is completely dependent upon the smart devices. The information retrieved from these devices should be spam free. The information retrieval from various IoT devices is a big challenge because it is collected from various domains. As there are multiple devices involved in IoT, so a large volume of data is generated having heterogeneity and variety. We can call this data as IoT data. IoT data has various features such as real-time, multi-source, rich and sparse.

Advantages

- The proposed scheme of spam detection is validated using five different machine learning models.
- An algorithm is proposed to compute the spam city score of each model which is then used for detection and intelligent decision making.
- Based upon the spam city score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.

4.OUTPUTSCREENS

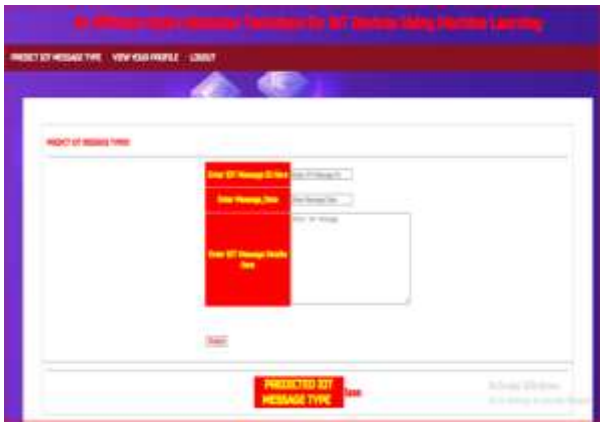


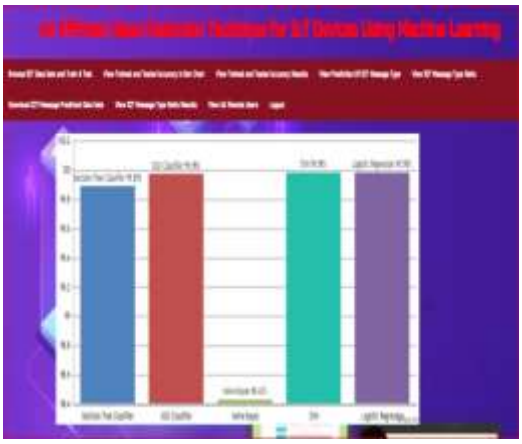


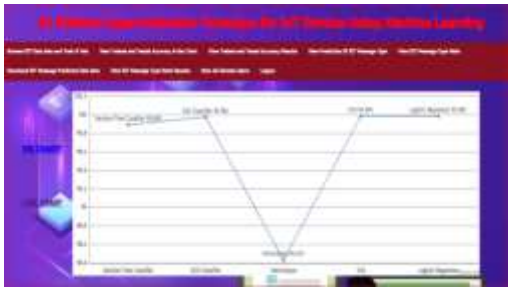
International Journal of Information Technology & Computer Engineering

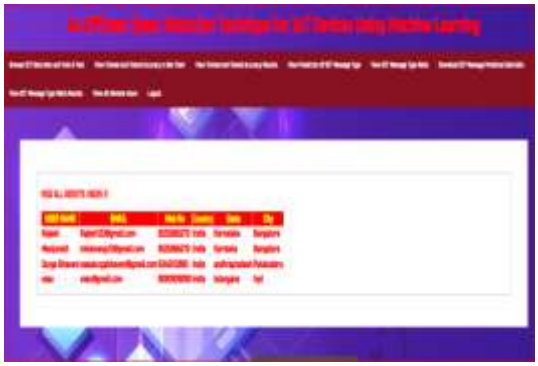
ISSN 2347–3657

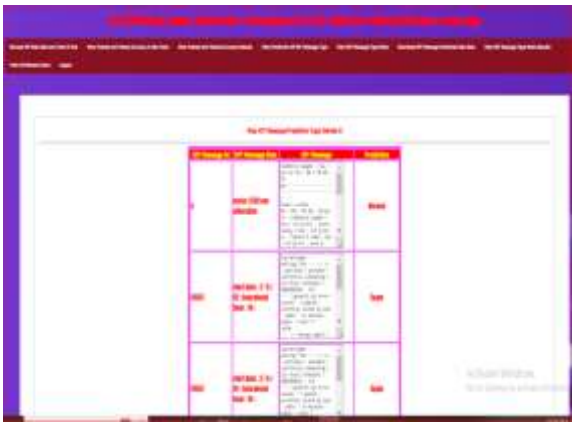
Volume 12, Issue 3, 2024





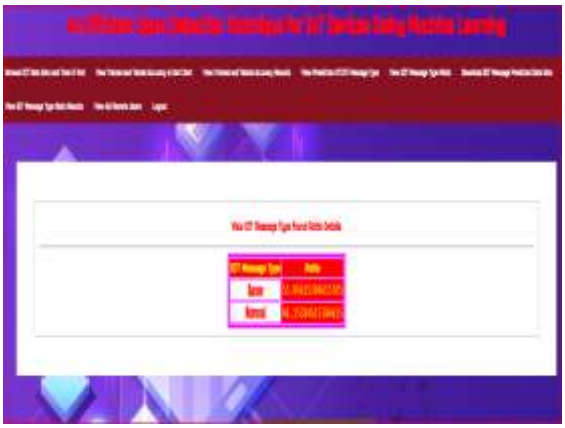


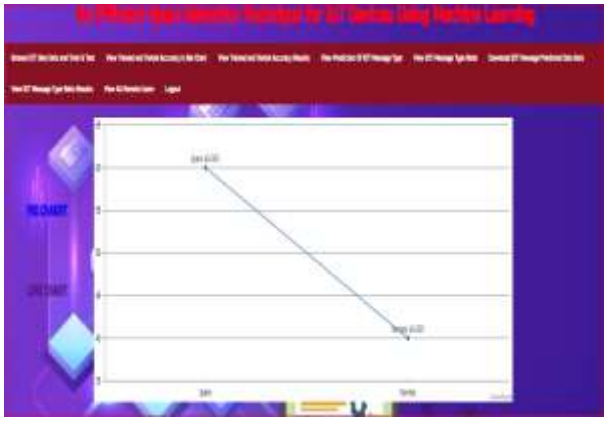




ISSN 2347–3657

Volume 12, Issue 3, 2024





5.CONCLUSION

The proposed framework, detects the spam parameters of IoT devices using machine learning models. The IoT dataset used for experiments, is preprocessed 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.

REFERENCES

1.Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, andS. Shieh, “Iot security: ongoing challenges and research opportunities,”in 2014 IEEE 7th international conference on service-oriented computingand applications. IEEE, 2014, pp. 230–234.

2.A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Block chain foriot security and privacy:

The case study of a smart home,” in 2017 IEEEInternational conference on pervasive computing and communicationsWorkshops (PerCom workshops). IEEE, 2017, pp. 618–623.

3. E. Bertino and N. Islam, “Botnets and internet of things security, Computer, no. 2, pp. 76–2017.

4.C. Zhang and R. Green, “Communication security in internet of thing: preventive

measure and avoid dos attack over iot network," in Proceedingsof the 18th Symposium on Communications & Networking. Societyfor 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 securityprotocol 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 basedsecure media access control protocol for wireless sensor networks," in2009 International Joint Conference on Neural Networks. IEEE, 2009,pp. 1680–1687.

8. M. A. Alsheikh, S. Lin, D. Niyato, and H.-P. Tan, "Machine learningin 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.