International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

A NOVEL MACHINE LEARNING FRAMEWORK FOR EFFICIENT SPAM DETECTION IN IOT SYSTEMS

[1]M.Mounika,[2]Chitla Sravya
[1]Assistant Professor, Depatment of MCA, Sree Chaitanya College of Engineering, Karimnagar
[2]MCA Student, Depatment of MCA, Sree Chaitanya College of Engineering, Karimnagar

ABSTRACT

Millions of devices with sensors and actuators connected via wired or wireless channels for data transfer make up the Internet of Things (IoT). Over the last ten years, the Internet of Things has expanded quickly, and by 2020, it is anticipated that over 25 billion gadgets will be connected. In the upcoming years, the amount of data that these gadgets disclose will grow significantly. The IoT devices generate a lot of data with a variety of modalities and differing data quality based on their speed in terms of time and position dependency, in addition to the increasing volume. In such a setting, machine learning algorithms can be crucial for biotechnology-based authorisation and security, as well as for detecting anomalies to enhance the security and usability of Internet of Things systems. Attackers, on the other hand, frequently use learning algorithms to take advantage of weaknesses in intelligent IoT-based systems. Inspired by this, we suggest in this work that machine learning be used to detect spam in order to secure IoT devices. A machine learning framework for spam detection in the Internet of Things is suggested in order to accomplish this goal. This system uses a vast collection of input feature sets and a variety of criteria to assess five machine learning models. The enhanced input characteristics are taken into account when each model calculates a spam score. This score shows how reliable an IoT device is based on a number of factors. The suggested method is validated using the REFIT Smart Home dataset. The outcomes demonstrate the suggested scheme's efficacy when compared to other current systems.

I. INTRODUCTION

The Internet of Things (IoT) makes it possible for real-world items to implement and merge regardless of their geographical locations. Privacy and protection measures are crucial yet difficult to implement in such a network management and control environment. To resolve security threats such intrusions, spoofing attacks, DoS attacks, jamming, eavesdropping, spam, and malware, IoT applications must safeguard user privacy. IoT device safety precautions vary depending on the size and kind of organisation using them.

The security gateways are forced to collaborate by user behaviour. Stated differently, the location, kind, and use of IoT devices determine the security measures [1]. For example, the smart organization's IoT security cameras can record various metrics for analysis and intelligent decision-making [2]. Since the majority of IoT devices are online dependant, the utmost caution should be used with web-based devices. It is typical in the workplace for IoT devices to be effectively utilised for implementing security and privacy features.

For instance, wearable technology should protect privacy by collecting and transmitting user health data to a linked smartphone. According to market research, 25–30% of active workers link their personal IoT devices to the company network. Both consumers and attackers are drawn to the IoT because of its growing scope. However, IoT devices adopt a defensive approach and determine the crucial parameters in the security protocols for the trade-off between security, privacy, and computation as a result of the advent of machine learning in various attack scenarios. Since an IoT system with limited resources typically finds it difficult to estimate the current network and timely attack state, this job is arduous.

II. LITERATURE SURVEY

IoT Security: Ongoing Challenges and Research Opportunities

The Internet of Things (IoT) opens opportunities for wearable devices, home appliances, and software to share and communicate information on the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected. In this paper, we begin with general information security background of IoT and continue on with information security related challenges that IoT will encountered. Finally, we will also point out research directions that could be the future work for the solutions to the security challenges that IoT encounters.

Blockchain for IoT security and privacy

Internet of Things (IoT) security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Blockchain-based approaches provide decentralized security and privacy, yet they involve significant energy, delay, and computational overhead that is not suitable for most resource-constrained IoT devices. In our previous work, we presented a lightweight instantiation of a BC particularly geared for use in IoT by eliminating the Proof of Work (POW) and the concept of coins. Our approach was exemplified in a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home. In this paper we delve deeper and outline the various core components and functions of the smart home tier. Each smart home is equipped with an always online, high resource device, known as “miner” that is responsible for handling all communication within and external to the home. The miner also preserves a private and secure BC, used for controlling and auditing communications. We show that our proposed BC-based smart home framework is secure by thoroughly analysing its security with respect to the fundamental security goals of confidentiality, integrity, and availability. Finally, we present simulation results to highlight that the overheads (in terms of traffic, processing time and energy consumption) introduced by our approach are insignificant relative to its security and privacy gains.

Botnets and Internet of Things Security

Recent distributed denial-of-service attacks demonstrate the high vulnerability of Internet of Things (IoT) systems and devices. Addressing this challenge will

require scalable security solutions optimized for the IoT ecosystem.

III. SYSTEM ANALYSIS AND DESIGN

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 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.

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

- 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 Supervised machine learning techniques is absence.

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

1) The proposed scheme of spam detection is validated using five different machine learning models.

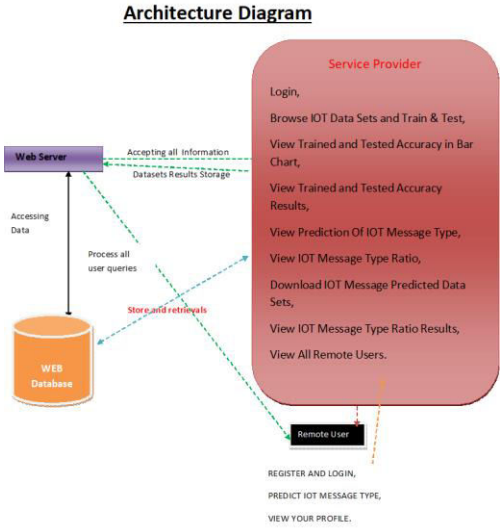
2) An algorithm is proposed to compute the spamicity score of each model which is then used for detection and intelligent decision making.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

3) Based upon the spamicity score computed in previous step, the reliability of IoT devices is analyzed using different evaluation metrics.

IV. SYSTEM DESIGN

SYSTEM ARCHITECTURE



V. SYSTEM IMPLEMENTATION

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse IOT Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View Prediction Of IOT Message Type, View IOT Message Type Ratio, Download IOT Message Predicted Data Sets, View IOT Message Type Ratio Results, View All Remote Users.

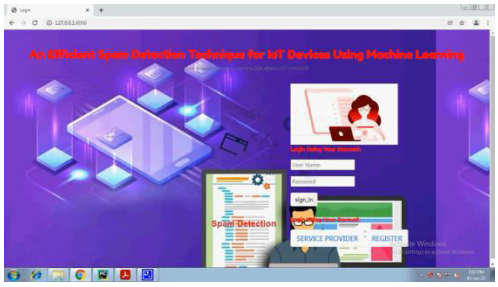
View and Authorize Users

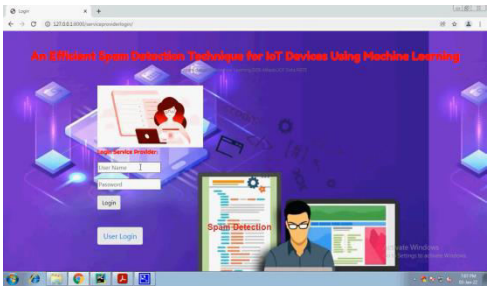
In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

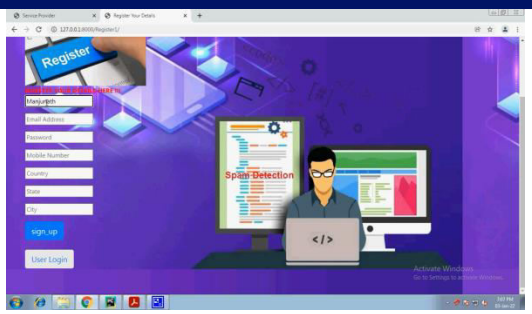
In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT IOT MESSAGE TYPE, VIEW YOUR PROFILE.

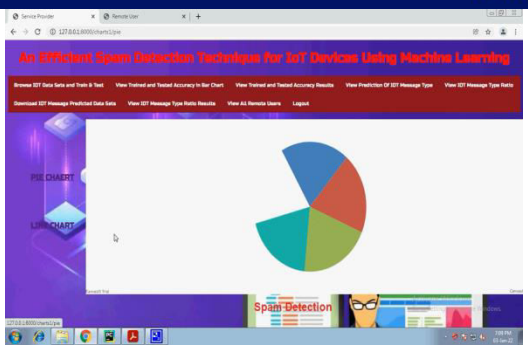
VI. SCREEN SHOTS

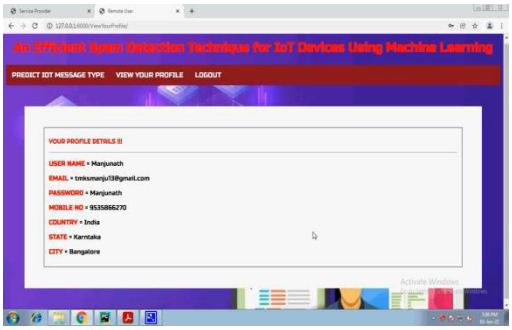


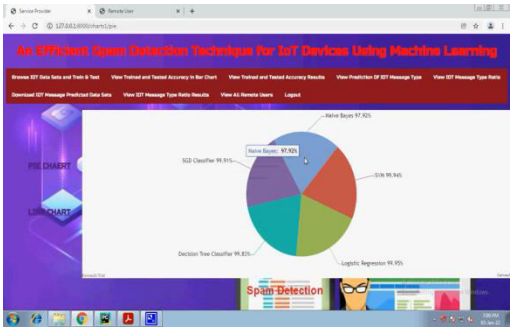


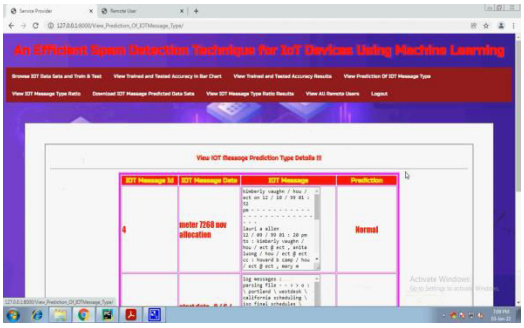
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

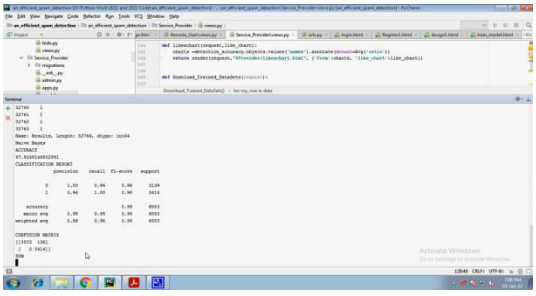


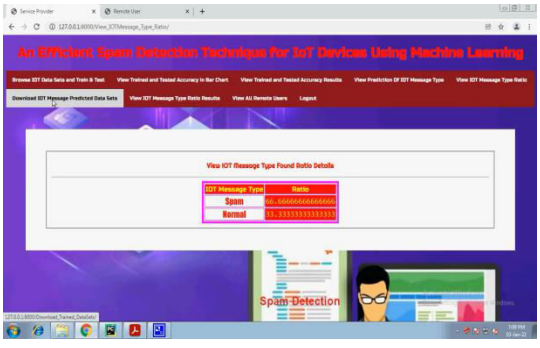




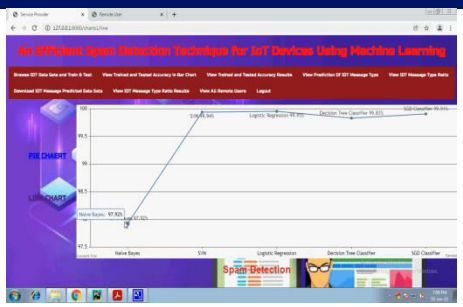


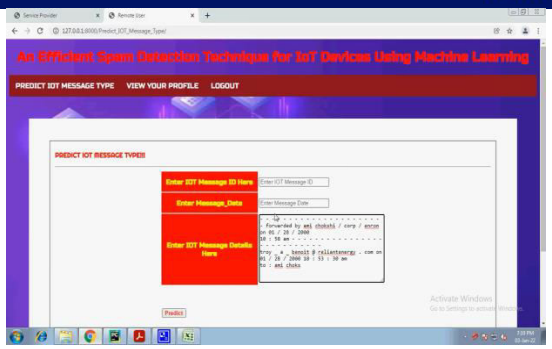


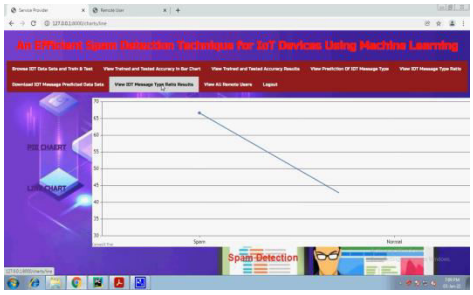


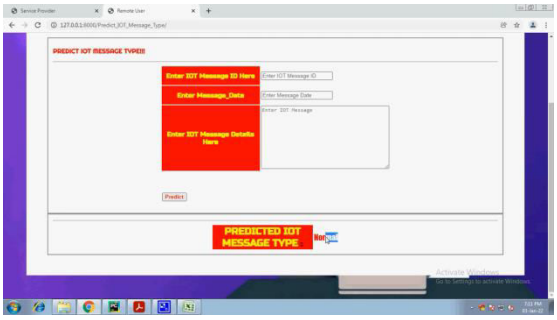


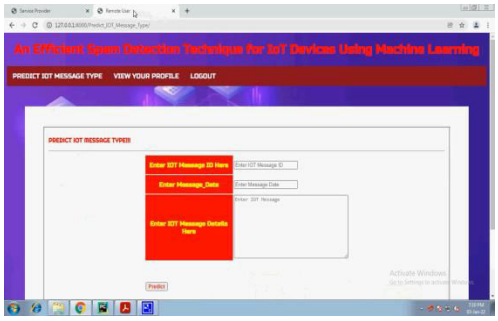
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

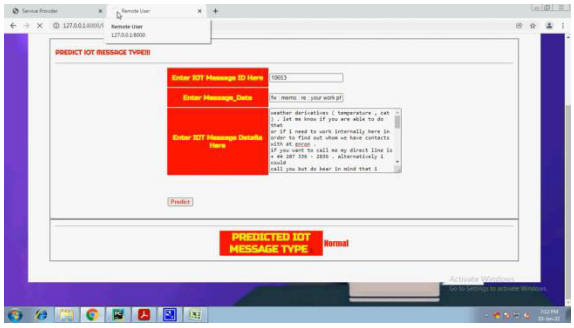


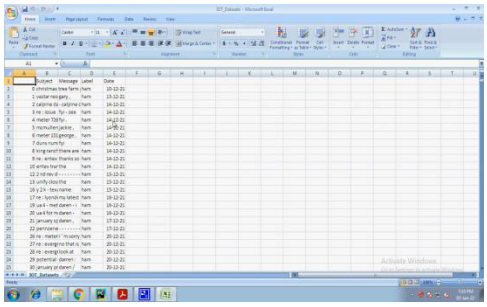


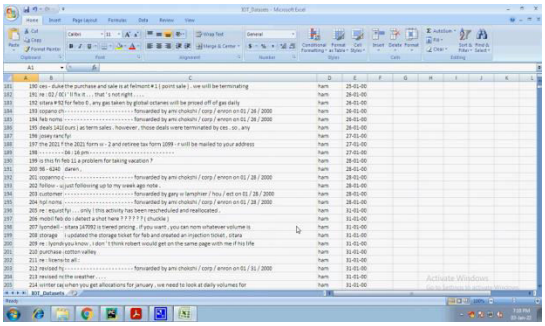












VII. CONCLUSIONS

The suggested system uses machine learning models to identify the spam parameters of Internet of Things devices. The feature engineering approach is used to preprocess the IoT dataset utilised in the tests. Every IoT device is given a spam score by experimenting with machine learning models within the framework. This improves the prerequisites needed for IoT devices to function properly in a smart home. We intend to take into account the climate and environmental aspects of IoT

devices in the future to make them more reliable and safe.

REFERENCES

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

[2] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). IEEE, 2017, pp. 618–623.

[3] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, no. 2, pp. 76–79, 2017.

[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] 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.

[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.

[19] A. H. Sodhro, Z. Luo, G. H. Sodhro, M. Muzamal, J. J. Rodrigues, and V. H. C. de Albuquerque, "Artificial intelligence based qos optimization for multimedia communication in iov systems," Future Generation Computer Systems, vol. 95, pp. 667–680, 2019.

[20] L. University, "Refit smart home dataset," https://repository.lboro.ac.uk/ articles/REFIT Smart Home dataset/2070091, 2019 (accessed April 26, 2019).

[21] R, "Rstudio," 2019 (accessed October 23, 2019).